U.S. DEPARTMENT OF THE INTERIOR

OFFICE OF SURFACE MINING

RECLAMATION AND ENFORCEMENT

DIRECTIVES SYSTEM

Subject Number:
IT-1

Transmittal Number:
889

Date: Mar 20, 2000

Subject:

Information Systems Security Program

Approval: /s/ Kathy Karpan Title: Director

1. Purpose. This Directive sets forth the policy for implementation of the Information Systems Security Program for the Office of Surface Mining (OSM). The program handbook identifies responsibilities and actions required of OSM personnel to assure an effective information systems security program.

2. Summary of Changes.

a. OSM is responsible for implementing and administering an Information Systems Security Program to protect its information resources, in compliance with the Computer Security Act of 1987 and the directives of the Office of Management and Budget, the National Security Agency, and other Federal agencies. To meet these requirements, OSM has instituted a formal Information Systems Security Program.

b. This program applies to all OSM organizations and their employees, including contractors, who are responsible for systems or data, both in hard copy or electronic form, or for the acquisition, management, and/or use of information resources. The program applies to all Information Systems, including application systems and databases; to all Information System facilities, including minicomputer and microcomputer platforms; Local Area Networks and Wide Area Networks.

c. The Information Systems Program Handbook is a policy document. In the interest of clarification, guidance and examples of standard processes and procedures are sometimes provided.

3. Definitions

a. Definitions - There are a multitude of definitions used within this handbook. A complete listing of official definitions and definitions for terminology and concepts used in this handbook can be found at Appendix B.

b. Acronyms - Appendix C of the handbook lists the definition of all acronyms used.

4. Policy/Procedure.

a. Policy. The procedures set out in the handbook are to be followed unless waivers are approved by the Director, OSM in writing.

b. Responsibilities.

(1) Assistant Director, Finance and Administration (AD, F&A) ensures that the procedures in this handbook are followed for information systems security program actions initiated in Headquarters, and

coordinates any waiver requests.

(2) Regional Director, Regional Coordinating Center ensures that the procedures in this handbook are followed for Information Systems Security Program operations initiated in the coordinating centers, field offices, and area offices.

c. Procedures.

(1) Requests for approval of waivers to this directive must be submitted on a case-by-case basis by memorandum through Chief, Division of Information Systems Management (ISM), to the AD, F&A. The Chief, ISM will evaluate the waiver request and will make recommendations to the Assistant Director, F&A, who will advise the Director. The Chief, ISM will coordinate with the Security Review Team where applicable.

(2) Recommendation for changes in the handbook must be submitted by memorandum to Chief, ISM. The handbook will be updated on an as-needed basis to incorporate any changes.

5. Reporting Requirements. None.

6. Effects on other documents. Directive INF-11, Information Resources Management Policies and Procedures Manual, Chapter II, G, "Information Resources Security Program" is rescinded.

7. References.

a. Departmental Manual 375 DM 19, DOI Security Manual.

b. Departmental Manual 441 DM 1-6, Personnel Suitability and Security Investigation Requirements.

c. Departmental Manual 444 DM 1, Physical Protection and Building Security.

d. Computer Crime Act of 1984.

e. Computer Security Act of 1987.

(See Appendix A of the Handbook for a complete list of all associated reference publications.)

8. Effective Date. Upon Issuance.

9. Contact. Louis Blasiotti, Information Systems Security Manager, (202) 208-2910.

10. Keywords. Information Systems Security Program Handbook.

INFORMATION

SYSTEMS SECURITY PROGRAM

HANDBOOK

Table of Contents

Chapter I. IS Security Program

Chapter II. Security Designations

Chapter III. Security Requirements

Chapter IV. Risk Management

Chapter V. Security Program Plan

Chapter VI. Contingency Planning

Chapter VII. Personnel Security/Suitability and Training

Chapter VIII. IT Facilities

Chapter IX. Integrating Computer Security into the System Life Cycle

Chapter X. Desktop, Software and Systems

Chapter XI. Data Communications, Networks, E-Mail, Servers and WAN

Chapter XII. Malicious Software and Intrusions

Appendices

Chapter I. Security Program

A. Overview

The Office of Surface Mining (OSM) (also referred to as "the Bureau") is responsible for implementing and administering an information systems security program to protect its information resources, in compliance with the Computer Security Act of 1987 and the directives of the Office of Management and Budget (OMB), the National Security Agency (NSA), and other Federal agencies. To meet these requirements, the Bureau has instituted the Information Systems Security Program (ISSP).

The security applies to all OSM organizations and their employees, including contractors, who are responsible for systems or data, both in hard copy and electronic form, or for the acquisition, management, and/or use of information resources. The program applies to all Information Systems (ISs), including application systems and databases; to all IT facilities, including minicomputer and microcomputer platforms; Local Area Networks (LANs) and Wide Area Networks (WANs).

This *Security Program* is a policy document. In the interest of clarification, guidance and examples of standard processes and procedures are sometimes provided. The purpose of this chapter is to provide an overview of the *Program*. This chapter covers the Bureau's information system security policy and security responsibilities.

B. Automated System Security Policy

OSM will implement a Bureau-wide information system security program to assure that each designated automated sensitive information system has a level of security that is commensurate with the risk and magnitude of the harm that could result from the loss, misuse, disclosure, or modification of the information contained in the system. Each system's level of security must protect the confidentiality, integrity, and availability of the information. Specifically, this requires that:

1. Each designated sensitive automated information technology system have the appropriate technical, personnel, administrative, environmental, and telecommunications safeguards;

2. Information system security should be cost-effective; and

3. Each designated sensitive information system has a contingency or disaster recovery plan to provide continuity of operation.

C. Definitions and Acronyms

Appendix B contains official definitions and concepts used in this document. Appendix C contains definitions of acronyms.

D. Information System Security Program Content

In accordance with overall OSM policy the following minimum security management structure is established with requirements that must be fulfilled.

Program Responsibilities

1. Implement and maintain security program, including the preparation of policies, standards, and procedures, as appropriate.

2. Designate a staff member to serve as Site Information Systems Security Officer (SISSO). Information Systems Management Division has primary responsibility for the overall direction of the ISSP within the organization.

3. Assign responsibility for the security of each automated system, facility, LAN and WAN to the appropriate employee and ensure adequate training.

4. Provide adequate resources to implement and maintain a cost-effective security program.

5. Assign security level designations to all databases, application systems, automated systems, facilities, and LANS. (See Chapter II, "Security Designations")

6. Implement physical security policies.

Security Plans

7. Identify sensitive systems, and develop and implement Computer Systems Security Plans (CSSPs). Program managers (individuals responsible for administering OSM programs and activities) are responsible for creation and implementation of security plans and Risk Assessments for designated mission critical systems.

Applications Security

8. Establish guidance to ensure that appropriate administrative, physical, and technical safeguards are incorporated into all new IS applications and significant modifications to existing systems. Guidance for sensitive applications must include policies and responsibilities for the following:

   a. Defining and approving systems security requirements prior to programming.

   b. Conducting and approving design reviews and application systems tests of the security features of systems prior to systems implementation.

9. Establish a program for conducting periodic reviews and evaluations, and for certifying the adequacy of the security safeguards of each information system commensurate with its security level designation. Such reviews must be conducted at intervals not exceeding three years.

10. Ensure that contingency plans are developed, maintained, and tested.

All contracting officers and COTRs are responsible for assuring that all contractors involved in developing information systems for use by OSM, or in providing any other type of service for the Bureau in which Federal Information Processing (FIP) resources are used, agree to comply with the requirements of the OSM Information System Security Plan.

Federal Information Resources Management Regulation (FIRMR), Subpart 201-21.3, "Security and Privacy" prescribes policies and procedures regarding security of FIP resources, including privacy safeguards for those FIP resources that process information about individuals. It requires that a proper level of security be maintained for all FIP resources, including those maintained or provided by contractors.

Personnel Security

11. Establish safeguards to ensure that all personnel who have access to sensitive information systems have the required authorities and the appropriate level of computer/ADP position designations, background investigations, and security clearances, if necessary.

Information Technology Installations

12. Assign responsibility for conducting periodic risk analyses for each information technology facility and LAN. Such periods will not exceed five years.

13. Ensure that appropriate security requirements are included in specifications for the acquisition or operation of information technology facilities, LANS, equipment, software packages, or related services.

14. Ensure that contingency or disaster recovery plans provide for adequate continuity of operations.

Security Awareness and Training

15. Develop, implement, and evaluate an employee information systems security awareness and training program.

Reporting

16. Include OMB Circular A-130 APPENDIX III, security weaknesses in the annual A-123 reports to the President.

17. Develop and implement a security breach reporting system.

E. Responsibilities

1. Director of the Office of Surface Mining Reclamation and Enforcement

The Director is responsible for the implementation and administration of an information systems security program within OSM.

2. Chief Information Officer (CIO)

The CIO, as the Designated Information Resources Management (IRM) Official, is responsible for:

a. Overseeing the Bureau's information systems security program and approving associated policy.

b. Ensuring an appropriate level of protection for all Bureau information resources, whether retained in-house or under the control of contractors, including the establishment of physical, administrative, and technical safeguards.

c. Issuing security program requirements and guidelines for data, information systems, facilities, and LANs. This includes both physical and electronic security requirements.

d. Ensuring that Information Systems Management Division has primary responsibility for the overall direction of the ISSP within the organization.

e. Ensuring overall policy and coordination of the OSM Information System Security Training Program.

f. Ensuring Application System Reviews are conducted.

3. Deputy Chief Information Officer for Information Resources Management (DCIO), Assistant Directors (AD), Regional Directors (RD), and Program Managers (PM)

The **DCIO** is responsible for:

a. Developing a security policy for the Bureau.

b. Appointing the Bureau Information Systems Security Officer for the Bureau to assist in coordinating and evaluating the information systems security program.

c. Defining and establishing requirements for sensitive systems.

d. Preparing any report that may be required of the OSM in conjunction with OMB Circular A-130, Appendix III and the Computer Security Act of 1987.

e. Developing security procedures, standards, and guidance consistent with Bureau and Federal requirements.

The **DCIO, AD, RD**, and **PM** are responsible for:

a. Promoting and coordinating the Bureau-wide information systems security program activities.

b. Monitoring organizational security program activities by:

1. Reviewing an annual sample of security plans for sensitive systems

2. Evaluating safeguards used to protect major information systems.

c. Performing official security liaison activities with non-OSM Government organizations and private organizations or committees, as required.

d. Coordinating the information system security program with the OSM's Internal Controls Review to preclude fraud, waste, and abuse with regard to the Bureau's information resources, and to avoid duplication of effort across these programs.

e. Implementing security procedures, standards, and guidance consistent with Bureau and Federal requirements.

f. Ensuring Application System Managers develop, implement and maintain an approved security plan for sensitive systems.

g. Establishing and administering a Security Awareness and Training program.

h. Integrating the information system security program with the internal control requirements of OMB Circular A-123.

i. Ensuring that managers within their organizations are kept apprised of, and held accountable for, security control requirements.

j. Ensuring that security designations are assigned for information technology facilities and LANs under their control.

k. Ensuring that appropriate risk management programs are developed, implemented, and maintained for all information technology facilities under his/her jurisdiction. (Refer to FIPS PUBS 31 and 65 for additional guidance.)

l. Ensuring that appropriate contingency plans are developed, tested, and maintained within his/her organization.

m. Ensuring that an Application System Manager is appointed for each application system and a Database Manager is appointed for each database.

n. Ensuring compliance with all legal requirements concerning the use of commercial proprietary software; e.g., respecting copyrights and obtaining appropriate licenses.

o. Ensuring that appropriate safeguards are implemented to minimize the risk to information systems, information technology facilities, and LANs from malicious software and intrusions. (See Chapter XII, “Malicious Software and Intrusions.”)

p. Specifying, implementing, and reviewing procedures used to protect their LANs and operating systems, including the performance of risk analyses and the determination of minimum security requirements and safeguards. The minimum-security requirements and safeguards for all information technology facilities are outlined in Chapter III, C, "Matrix of Minimum Security Safeguards."

q. Ensuring that the organizations within their jurisdictions comply with the applicable personnel security provisions.

4. Information Security Officer Review Team (iSORT)

The Information Security Officer Review Team is responsible for:

a. Reviewing and evaluating all OSM automated systems and the IT security program.
b. Reporting to the CIO completed audits and reviews.
c. Preparing IT audit plan annually.
d. Insuring compliance by all OSM offices and individuals with all aspects of the IT security program.

5. Chief, Personnel Office (CPO)

The **CPO** is responsible for:

a. Ensuring that all positions, where the incumbent’s primary responsibilities involve the design, development, administration, or maintenance of computer systems are assigned appropriate computer/ADP designation.

b. Ensuring that the divisions have properly adjusted Low Risk Public Trust or National security positions designations to reflect the sensitivity level of the Information System accessed by the incumbent and the computer related responsibilities of the position.

c. Ensuring appropriate background checks are submitted on incumbents.

6. LAN Managers

LAN Managers are responsible for:

a. Ensuring the security of the data and application systems stored or processed in their LANs.

b. Ensuring that basic security services are provided for their information technology facilities; e.g., access, temperature control, fire protection, and electrical power.

c. Ensuring that appropriate security requirements are included in the specifications for the acquisition and operation of the LANs and related services.

d. Determining the level of secure service their information technology facilities/LANs are to provide, and assigning security level designations to their information technology facilities/LANs based on the sensitivity of the LANs and databases they need to process. (See Chapter VIII, “IT Facilities”.)

e. Specifying, implementing, and reviewing procedures used to protect the integrity of their information technology facilities/LANs and operating systems.

f. Ensuring that their IT facilities fully comply with physical security requirements.

g. Ensuring that the security procedures are continuously evaluated and monitored for security breaches and corrective action taken where necessary.

h. Ensuring that all IRM Coordinators and users of their information technology facilities/LANs are aware of the level of secure service offered, including safeguards that may be implemented and waivers received.

i. Conducting risk analyses of their information technology facilities/LANs to determine cost-effective and essential security safeguards. (See Chapter IV, “Risk Management.”) The minimum-security requirements and safeguards for all information technology facilities are outlined in Chapter III, C, “Matrix of Minimum Security Safeguards”.

j. Developing Computer Systems Security Plans (CSSPs) for communication systems or networks that transmit sensitive data.

k. Developing and maintaining contingency plans, including the designation of personnel to be responsible for effecting backup operations in the event of major disruptions. (See Chapter VI, “Contingency Planning,” and Chapter XI, “Data Communications and Networks, E-Mail, Servers and WANs.”)

l. Providing security for the data and application systems stored or processed in their information technology facilities/LANs.

m. Selecting, implementing, and maintaining safeguards that minimize the risk to their information technology facilities/LANs from malicious software and intrusions. (See Chapter XII, “Malicious Software and Intrusions.”)

7. Information Systems Security Officer (ISSO)

The ISSO is responsible for:

a. Managing the Bureau IS Security Program; coordinating all Bureau activities designed to protect IS resources; coordinating Bureau IS security training programs, and reporting on the effectiveness of these activities to Bureau and Departmental management.

b. Developing recommendations for Bureau policy for IS security; developing security procedures, instructions, guidelines and developing overall Bureau IS security goals and objectives.

c. Developing, implementing and maintaining a Bureau management plan that provides for the mandatory periodic training in IS security awareness and accepted IS security practices for all employees who are involved with the management, operation, or use of each Federal IS system within or under the supervision of the Bureau.

d. Ensuring the implementation of IS security plans, as required by the Computer Security Act of 1987, for general support systems and major application systems or systems containing sensitive data.

e. Maintaining a current inventory of general support and sensitive systems including a list of all users having access to these systems, major applications and systems containing sensitive data, and a schedule for testing sensitive system contingency plans.

f. Coordinating all pertinent IS security matters pertaining to physical and personnel security with the IS Security Officers.

g. Reviewing the IS security guidelines with other DOI bureaus and the Office of the Secretary.

h. Maintaining liaison with the Office of the Secretary, the DOI bureaus and other government agencies for the purpose of sharing information resources.

i. Coordinating and preparing reports required by the Department of the Interior and other agencies.

j. Scheduling an annual meeting of all SISSOs and other involved parties to be chaired by the DCIO.

8. Site Information System Security Officers (SISSO)

SISSOs are responsible for:

a. Directing, coordinating, and evaluating the information technology security of their organizations to protect an IT installation or any other technical system designated by management. Providing technical assistance to installation management on IS security requirements.

b. Evaluating and providing information about the security plan to the organization's management, and communicating Bureau requirements and concerns to the organization.

c. Ensuring that security plans for sensitive systems are developed, reviewed, implemented, and revised every three (3) years or when major changes are made to the system.

d. Providing advice and assistance to other Security Officers, Application Managers, LAN Managers, Facilities Management, and other organizational personnel concerning the security of sensitive data and the security of critical data processing capabilities.

e. Reporting information resources security breaches in accordance with the security breach reporting procedures developed and implemented by the Chief, Information Systems Management Division.

f. Coordinating the risk management programs of their organizations, assisting in approving the development of IS security plans, risk assessments in general support systems, major applications and systems containing sensitive data.

g. Maintaining the documentation used to establish the security level designations of all databases, application systems, information technology facilities, and LANs within their organizations.

h. Assisting Facilities Management and LAN Managers in developing policies to ensure that contingency plans are either in place for information technology facilities and LANs or are under active development. (See Chapter VI, "Contingency Planning.")

i. Ensuring the organization's compliance with the IS Personnel Security Program. (See Chapter VII, "Personnel Security/Suitability and Training.")

j. Assisting Application System Managers in establishing, and users in implementing, the appropriate security safeguards required to protect microcomputer hardware and data from improper use or abuse. (See Chapter X, "Desktop, Software, and Systems.")

k. Assisting Project Officers and appropriate Application System Managers/Facilities Management/LAN Managers in carrying out the provisions of the security policy for solicitations and contracts and for certifying that proposals received in response to an RFP and certified as winning proposals by the Project Officer, comply with the requirements of Bureau security.

l. Assisting Facilities Management and LAN Managers in selecting and implementing safeguards that minimize the risk to information systems, information technology facilities, and LANs from malicious software and intrusions. (See Chapter XII, "Malicious Software and Intrusions.")

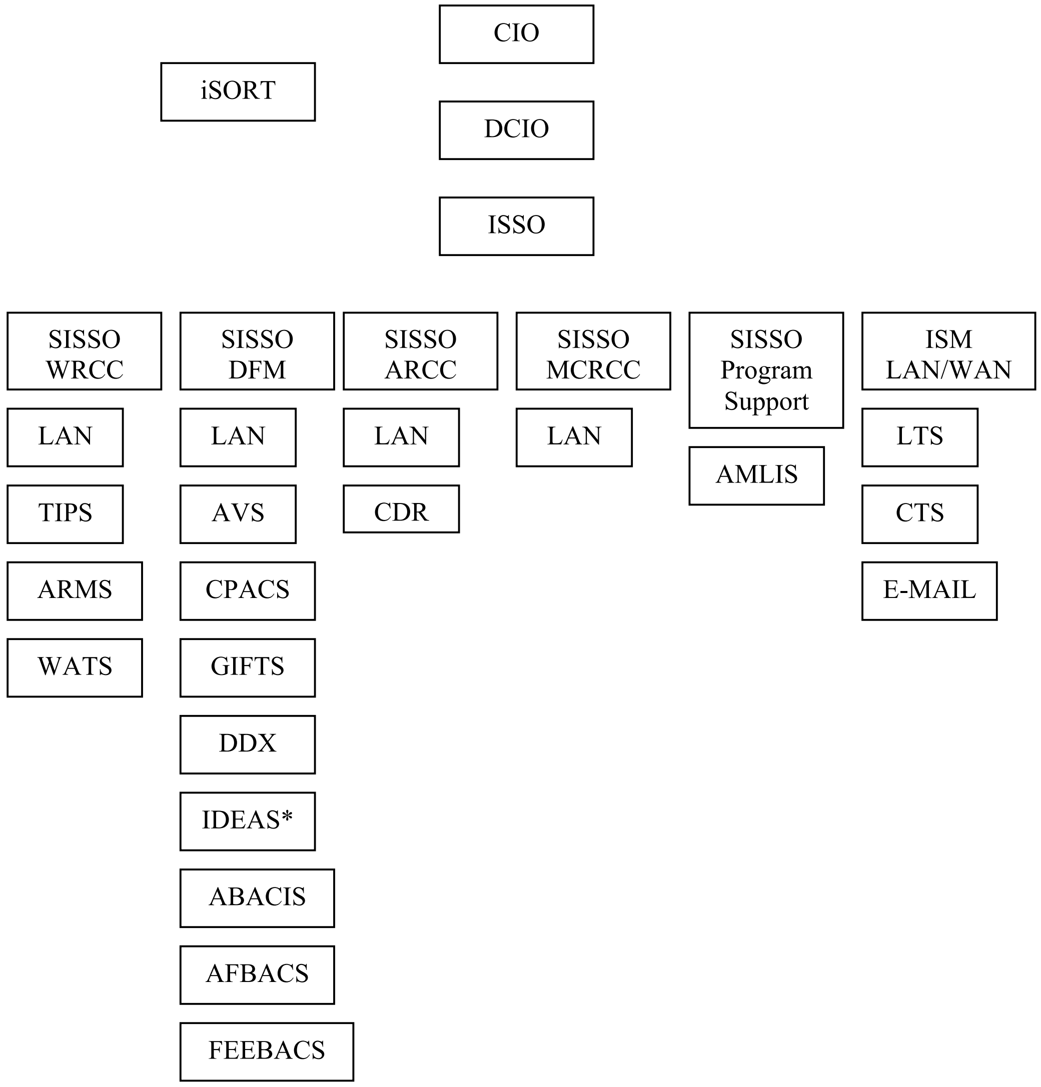
m. Making recommendations to management on the sensitivity of information technology related positions under their supervision. Making recommendations to ensure that all IRM positions are assigned a sensitivity level designation and that the Personnel Office staff is provided this information in accordance with 441 DM 1-6.

n. Ensuring that the current version of anti-virus software is loaded on Bureau workstations and servers.

o. Providing, on an on-going basis, IS security awareness training activities for Managers, Supervisors, LAN Managers, System Managers, technical staff and users.

p. Coordinating and maintaining liaison with the Bureau ISSO on all IT security matters.

Security Management Structure



* IDEAS replaced SATIN

9. System Managers and Application System Managers

System Managers are responsible for:

a. Ensuring the security of the data within their information systems, including the determination of the security designations for their associated databases. (See Chapter II, “Security Designations.”)

b. Ensuring that appropriate security safeguards exist to adequately protect their information systems (and databases for which they are responsible) commensurate with the security level designations assigned (e.g., secure storage facilities, duplicate backup copies, alternative "contingency processing plans"). (See Chapter II, “Security Designations.”)

c. Ensuring that the security requirements of their data and data processing capabilities will be or are being met.

d. Conducting risk analyses of their information systems to determine cost- effective and essential security safeguards. (See Chapter IV, "Risk Management.")

e. Ensuring that backup copies of data and applications critical to the performance of their organizations are made, maintained, safeguarded, and ready for use in the event of a disaster. (See Chapter VI, "Contingency Planning.")

e. Ensuring that all users of their information systems are trained in the use of safeguards and that they use these safeguards to protect the information system.

f. Approving access to their systems. (Note: In some locations this individual may be referred to as either the System Manager or the System Owner.)

Application System Managers are responsible for:

a. Reviewing that the security requirements of their application systems are being met or will be met.

b. Ensuring that appropriate administrative, physical, and technical safeguards are incorporated into application systems under development or enhancement. These safeguards include defining and approving security specifications, conducting design reviews of security features, testing security features, and protecting sensitive data during development.

Both System Managers and Application System Managers are responsible for:

a. Periodically reviewing and verifying that all users of their IS/application systems are authorized and are using the required security safeguards.

b. Working with the Project Officer, Contracting Officers, and organization Security Officer to ensure that Requests for Proposals (RFP) pertaining to their application systems comply with the security requirements, and participating in the technical review of proposals.

10. Database Managers

Database Managers are responsible for:

a. Designating the sensitivity levels of their databases and establishing and communicating the security safeguards required for protecting them. (See Chapter II, "Security Designations").

b. Notifying the ISSO, SISSO, and users of the level of security required by their databases.

c. Ensuring that the security requirements of their databases are being met or will be met for sensitive systems.

d. Documenting and explaining why required security safeguards or recommendations cited in Risk Assessments/CSSPs cannot be met.

e. Periodically reviewing and verifying that all users of their databases are authorized and are using the required security safeguards.

f. Ensuring that their databases are only run at approved information technology facilities and LANs

10. OSM Privacy Act Officer (PAO)/OSM Records Management Officer (RMO)

Privacy Act Officer (PAO) is responsible for the following activities:

a. Informing the ISSO when systems subject to the Privacy Act are reported to the PAO by the System Owner as undergoing significant changes.

b. Giving guidance to System Owners as to their responsibilities under the Privacy Act.

c. Coordinating a biennial review of all systems of records to verify compliance with the Privacy Act. System Owners and System Managers physically conduct this review.

d. Assisting the System Owner and System Manager in the preparation of the *Federal Register* notice for systems subject to the Privacy Act and the property of OSM.

Records Management Officer (RMO) is responsible for the following activities:

a. Providing guidance as to the required retention of all records in the control of the System Owner, Database Manager and End User.

b. Creating and distributing retention schedules for all electronic records, including databases, word processing documents, electronic mail and web pages.

c. Informing the ISSO, SISSOs Systems Managers, and Systems Owners of changes in electronic records lifecycle maintenance requirements promulgated by the National Archives and Records Administration.

d. Advising the Chief Information Officer on electronic records management issues.

11. Contracting Officers (CO)

Contracting Officers are responsible for:

a. Ensuring the contractor's compliance with all of OSM's systems security requirements.

b. Ensuring requirements from the Federal Acquisition Regulations are incorporated into all contracts.

Contracting Officer and the COTR are responsible for ensuring all contractors who are involved in developing information systems for use by OSM or in providing any other type of service for the Bureau in which Federal Information Processing (FIP) resources are used, must agree to comply with the requirements of the OSM Information System Security Program. *Federal Information Resources Management Regulation (FIRMR)* Subpart 201-21.3, "Security and Privacy," prescribes policies and procedures regarding security of FIP resources, including privacy safeguards for those FIP resources that process information about individuals. It requires that a proper level of security be maintained for all FIP resources, including those maintained or provided by contractors.

13. Supervisors

Supervisors are responsible for:

a. Ensuring that their employees are aware, and observe, all of the security requirements of the data, information systems, information technology facilities, LANs, and workstations they use.

b. Ensuring employees strictly adhere with all legal requirements concerning the use of proprietary software; e.g., respecting copyrights obtaining site licenses and proper Internet and E-mail usage.

c. Determining the appropriate position sensitivity designations for positions under their jurisdiction and ensuring that Employees under their jurisdiction have undergone appropriate background investigations. (See Chapter VII "Personnel Security/Suitability and Training.")

d. Ensuring that employees receive appropriate security training.

e. **Contacting immediately the E-mail account "Clearance" for notification of all systems managers whenever an employee transfers, is reassigned, no longer requires access, or is separated from OSM.**

14. IT Facility/Telecommunications Managers

IT Facility/Telecommunications Managers are responsible for safeguarding the data communications equipment and software under their control. If any of this equipment or software is under the control of more than one of these individuals, then the Deputy CIO is to designate a single responsible individual. The individuals in control are responsible for:

a. Developing and maintaining a functional diagram or flow chart of the data communications network which:

1. Shows the method of interconnection within the network, such as couplers and hard-wired and dial-up lines;

2. Indicates transmission speeds and software protocols.

b. Conducting a risk analysis and associated cost-benefit analysis to determine the type and relative importance of protection needed for the data communications network.

c. Determining the security level designation for the data communications network.

d. Establishing and implementing required and appropriate procedures, controls, and security safeguards for the data communications network.

e. Warning potential intruders that Federal systems are for the use of authorized users only.

f. Developing a Computer Systems Security Plan (CSSP) for any communications systems or networks that transmit sensitive data.

g. Developing and maintaining a contingency plan for use in the event of major disruptions to the communication of highly sensitive data or highly critical data communications capabilities. The contingency plan should include testing, evaluation, and modification to the extent feasible.

h. Conducting periodic internal control reviews of the security of the data communication network.

i. Selecting, implementing and maintaining safeguards that minimize the risk to IT facilities and Networks from malicious software and intrusions.

15. Users

Users are responsible for:

a. Assisting in the development of contingency plans. This responsibility particularly involves determining which parts of automated processes can revert to manual processing and which parts need priority automated processing.

b. Using all of the security measures available to protect application system databases.

c. Assisting Application System/Database Managers in determining the required security designations for application systems/databases.

d. Assisting Application System Managers in defining security specifications and testing security features of application systems under development or being enhanced.

e. Running application systems/databases only at authorized information technology facilities and LANs that are designated at a level of security equal to or higher than the security designated for their application systems/databases.

f. Implementing specified security safeguards to prevent fraud, waste, or abuse of the hardware, application systems, and data they are authorized to use.

g. Conforming to security policies and procedures that minimize the risk to automated systems, information technology facilities, and LANs from malicious software and intrusions (See Chapter XII, "Malicious Software and Intrusions.")

h. Complying with OSM's E-mail and Internet policies.

i. Ensuring that only authorized software runs on government computers and other government hardware.

j. Conforming to security policies and procedures that minimize the risk to OSM systems, and IT Facilities and Networks from malicious software and intrusions.

All users are responsible for assisting in the protection of the Bureau's automated correspondence, data, systems, and equipment by complying with the security requirements contained in this Handbook. Employees may not run unauthorized software programs on the Bureau's computers and must comply with all copyright requirements.

Chapter II. Security Designations

A. Overview

The security efforts of the Information Systems Security Program (ISSP) are based on the sensitivity of data contained in Information Systems (ISs) and the operational criticality of the data processing capabilities of automated systems. Security designations are used to define the requirements of these security efforts. System Managers are responsible for identifying the appropriate security designations for their information systems. System Managers should use NIST 800-18 in determining required security levels.

B. Introduction to Security Designations

The security designations are based on:

1. The *sensitivity of data*; i.e., the need to protect data from unauthorized disclosure, fraud, waste, or abuse; and

2. The *operational criticality of data processing capabilities*; i.e., the ramifications if data processing capabilities were interrupted for a period of time or subject to fraud or abuse.

There are three security designations for data sensitivity and for operational criticality. The Systems Manager should consider each system from both points of view, then choose the higher rating for the overall security designation.

An information system may be compartmentalized, such that a given data set or process is more sensitive than other data sets or processes. The Systems Manager should assign the highest security designation of any data set or process within the information systems for the overall security designation. This practice supports the Confidentiality, Integrity, and Availability (CIA) security requirements defined by the Office of Management and Budget (OMB):

> **Confidentiality -** The system contains information that requires protection from unauthorized disclosure.
>
> **Integrity -** The system contains information that must be protected from unauthorized, unanticipated, or unintentional modification, including the detection of such activities.
>
> **Availability -** The system contains information or provides services that must be available on a timely basis to meet mission requirements or to avoid substantial losses.

System Managers must ensure that their databases and the processing capabilities of their information systems are accessed only by authorized users who fully utilize the required security safeguards. The managers of compartmentalized information systems should take special care to specify the appropriate level of security required.

To summarize, the OSM's security designations determine the minimum-security safeguards required to protect sensitive data and to ensure the operational continuity of critical data processing capabilities. **Managers in conjunction with applicable System Owners and others should use a combination of the sensitive and criticality attributes to determine an overall level of sensitivity. Systems are rated non-sensitive or sensitive.**

C. Sensitivity for Databases

Sensitivity designations are assigned to databases based on the type of data in the database and the requirements of specific laws governing the protection or disclosure of information; e.g., the Privacy Act.

1. Low Sensitivity

This category identifies data that require minimal protection. Threats to these data are minimal, and only minimal precautions to protect the data need to be taken at the user site. Accidental alteration or destruction is the primary concern for these types of data. This category includes:

a. Databases that have value to a researcher only in their raw form, such as in some laboratory research applications, and the computerized correspondence and documents in some offices.

b. Automated systems of records subject to the Privacy Act, which contain information that is virtually all in the public domain, such as employee locator files, and for which any unauthorized disclosures could reasonably be expected not to adversely affect the individual.

2. Moderate Sensitivity

This category identifies data that have some importance to the OSM and which must be protected against such acts as malicious destruction. However, since these types of data are most often collected for analytical purposes, disclosure problems are not usually significant. This category includes:

a. Management information concerning workload, performance, staffing, and similar data, usually in statistical form, used to generate reports that reflect the status of an organization. Access to these data needs to be restricted only to a limited degree. The data are protected because of their value to the organization, but they are intended to be disclosed in some form eventually.

b. Research and statistical data accumulated to provide information about OSM programs to the public. These data need protection commensurate with the value of the information to the organization. Loss of this kind of data would not normally be potentially embarrassing or detrimental either to an individual or to the organization.

c. Automated systems of records subject to the Privacy Act, which contain information not in the public domain, but for which unauthorized disclosure could cause nonspecific embarrassment to an individual.

d. Computerized correspondence and documents, which must be protected from unauthorized alteration or disclosure. These types of data include all correspondence, memoranda, and other documents whose release or distribution outside the Federal Government and/or within the organization needs to be controlled.

3. High Sensitivity

This category contains the most sensitive unclassified data (other than unclassified data whose loss could adversely affect national security interests). The data in this category require the greatest number and most stringent security safeguards at the user level. This category includes:

a. Payment information that is used to authorize or make cash payments to individuals or organizations. These data are usually stored in production application files and systems, and include benefits information, such as that found at the Social Security Administration (SSA), and payroll information. Such information also includes databases that the user has the authority and capability to use and/or alter to cause an improper payment.

b. Proprietary information that has value in and of itself and which must be protected from unauthorized disclosure.

c. Computerized correspondence and documents that are considered highly sensitive and/or critical to an organization and which must be protected from unauthorized alteration and/or premature disclosure.

d. Automated systems of records subject to the Privacy Act, which contain information that meets the qualifications for Exemption 6 of the Freedom of Information Act; i.e., for which unauthorized disclosure would constitute a "clearly unwarranted invasion of personal privacy" likely to lead to specific detrimental consequences for the individual in terms of financial, employment, medical, psychological, or social standing.

D. Criticality for Application Systems

Criticality levels are assigned to information systems based upon the relative importance of their processing capabilities to the organizations they support. A low designation is used for an information system with the lowest criticality of data processing relative to the organization it supports; and a high designation is used for an information system with the highest criticality.

1. Low Criticality

This category identifies information systems with data processing capabilities that require minimal protection. These include information systems that, in the event of alteration or failure, would affect the organization minimally or could be replaced with a minimum of staff time or expense. This category also includes information systems that generate, store, process, transfer, or communicate data. These information systems are considered to have low or no sensitivity.

2. Moderate Criticality

This category identifies automated systems with data processing capabilities that are considered important but not critical to the internal management of an organization and/or the Bureau. This category includes:

a. Information systems whose failure to function for an extended period of time would not have a critical impact on the organizations they support.

b. Information systems that generate, store, process, transfer, or communicate data that are considered to have moderate sensitivity.

3. High Criticality

This category identifies information systems with data processing capabilities that are considered critical to the organizations they support and/or the Bureau. This category includes:

a. Information systems whose failure to function for even a short period of time could have a severe impact on the organizations they support and/or the Bureau.

b. Information systems that perform functions with data that are considered to have a high potential for fraud, waste, or abuse.

c. Information systems that generate, store, process, transfer, or communicate data that are considered to have high sensitivity.

Chapter III. Security Requirements

A. Overview

This chapter outlines the minimum security requirements for non-sensitive and sensitive systems. The security requirements apply to all information technology facilities and LANs under the jurisdiction of OSM, including those that are operated by government agencies other than OSM and by contractors functioning as agents of OSM.

The higher the security level designation of an information system, information technology facility, or LAN, the more stringent its security requirements. Information technology facilities and LANs with the lowest security level designations usually require only ordinary security precautions; i.e., protection by safeguards which are considered to be good management practice. In all instances, the minimum security requirements of information systems facilities and LANs should be equal to or higher than the highest Security level designation of any data they process, including data received from other agencies.

There are many possible methods for manipulating on-line systems. System Managers, Information Technology Facility and LAN Managers must continually evaluate their systems to determine whether they can be circumvented, and must test their security safeguards to ensure that they are functioning as intended. A review is required at least once every three years. Additional reviews are required if the safeguard requirements outlined in this chapter change or if an information system, information technology facility or LAN undergoes a significant modification. A waiver must be requested prior to review if an information system, information technology facility or LAN is not in compliance and cannot be brought into compliance in a relatively short period of time.

B. Security Requirements

1. Non-sensitive

The controls required to adequately safeguard a non-sensitive systems are those which would normally be considered good management practice. These include, but are not limited to:

a. An employee information systems security awareness and training program.

b. The assignment of sensitivity designations to every employee position and any background investigation.

c. Physical access controls.

d. A complete set of information systems documentation.

e. Record retention procedures.

f. A list of authorized users.

2. Sensitive

The controls required to adequately safeguard a sensitive system include all of the requirements for non-sensitive systems, plus the following requirements:

a. A detailed risk management program.

b. A security plan for systems processing sensitive information.

c. Security review.

d. Required background investigations for employees based on position sensitivity.

e. Required background investigations for contractor personnel.

f. A formal written contingency plan.

g. A formal risk assessment.

h. An automated audit trail.

i. Authorized access and control procedures.

j. Secure physical transportation procedures.

k. Secure telecommunications.

l. An uninterrupted power supply.

C. Matrix of Minimum Security Safeguards

A Matrix of Minimum Security Safeguards identifies the safeguards that are required to protect all types of information systems, information technology facilities, and LANs. An "X" on the matrix means that a security safeguard is a requirement for an information systems and information technology facility, or LANs with that security designation, and an "O" on the matrix means that the security safeguard is optional. It is important to note that the security safeguards are minimum requirements. They should be augmented based on the data sensitivity and operational criticality of the information system, information technology facilities or LANs.

Matrix of Minimum Security Safeguards		
	Security Level	
	Sensitive	Non-Sensitive
1. Ensure that a complete and current set of documentation exists for all operating systems.	X	X
2. Require use of current passwords and log-on codes to protect sensitive IS data from unauthorized access.	X	0
3. Establish procedures to register and protect secrecy of passwords and log-on codes, including the use of a non-print, non-display feature.	X	0
4. Limit the number of unsuccessful attempts to access an IS or a database.	X	0
5. Develop means whereby the user's authorization can be determined. (This may include answer back capability.)	X	0
6. Establish an automated audit trail.	X	0
7. Implement methods, which may include the establishment of encryption, to secure data being transferred between two points.	X	0
8. Ensure that the operating system contains controls to prevent unauthorized access to the executive or control software system.	X	0
9. Ensure that the operating system contains controls that separate user and master modes of operations.	X	0
10. Record occurrences of non-routine user or operator activity (such as unauthorized access attempts and operator overrides) and report to the organizational SISSO.	X	0
11. Install software feature(s) that will automatically lock out the user account if it is not used for a predetermined period of time.	X	0
12. Establish controls over the handling of sensitive data, including labeling materials and controlling the availability and flow of data.	X	0
13. Require that all sensitive material be stored in a secure location when not in use.	X	0
14. Prepare and maintain list of persons authorized to access information technology facilities and IS processing sensitive data.	X	0
15. Establish procedures for controlling access to facilities and ISs processing sensitive data.	X	X
16. Furnish locks and other protective measures on doors and windows to prevent unauthorized access to computer and support areas.	X	X
17. Specify fire-rated walls, ceilings, and doors for construction of new computer facilities or modifications of existing facilities.	X	0
18. Install smoke and fire detection systems with alarms in the computer facility.	X	0
19. Provide emergency power shutdown controls to shut down IS equipment and air conditioning systems in the event of fire or other emergencies.	X	X
20. Provide waterproof covers to protect computers and other electronic equipment from water damage.	X	0

21. Establish a fire emergency preparedness plan to include training of fire emergency response teams, development and testing of an evacuation plan, and on-site orientation visits for the local fire Department.	X	X
22. Establish detailed risk management program.	X	0
23. Establish Computer Systems Security Plans for sensitive systems.	X	X
24. Establish employee security awareness and training programs.	X	X
25. Maintain accurate inventory of all hardware and software.	X	X
26. Establish security review.	X	X
27. Establish contingency plan.	X	X
28. Install Uninterrupted Power Supply (UPS).	X	0
29. Ensure that all personnel positions have been assigned security level designations.	X	X
30. Conduct periodic security designation reviews.	X	0
31. Ensure that all personnel, including contractors, have received appropriate background investigations.	X	0
32. Maintain a list of all personnel, including contractors, who have been approved for High and Moderate Positions and National Security Positions. (See Chapter VII, “Personnel Security/Suitability and Training.”)	X	X

Chapter IV. Risk Management

A. Overview

To ensure appropriate safeguards for mission-critical information systems, databases with sensitive and politically sensitive data and LANs, all OSM organizations must develop, implement, and maintain risk management programs to ensure that appropriate safeguard measures are taken to protect all data, information technology facilities, and LANs. All systems identified as sensitive will have corresponding security plans in place.

The purpose of this chapter is to describe the basic elements of a successful risk management program at the organizational level. Although the specific characteristics of each risk management program may vary, the general principles and methods of risk management remain the same. All risk management programs consist of a risk assessment followed by safeguard selection and implementation.

B. Risk Management Program

Each OSM organization must develop a comprehensive risk management program for mission-critical information systems, sensitive data, high profile “political systems” and LANs. It is impossible to eliminate risk completely. Managers need to be aware of the potential risks and vulnerabilities to data, information technology facilities, and LANs. Once they are aware of the vulnerabilities, the potential risks, and the potential safeguard options, management can then make informed decisions concerning the necessity and cost-benefit of the various security alternatives/safeguard options.

A risk assessment of sensitive information systems is required at least once every three years. Facilities and networks must be reviewed every five years. Additional reviews are required whenever a system, facility, or network undergoes a significant modification.

Use of an automated risk assessment application package can allow responsible managers to conduct assessment more frequently, and offer a cost-benefit approach to risk management. If a risk assessment shows lack of compliance with security safeguards (see Chapter II, "Security Designation"), the reasons why the security requirements cannot be met must be documented, and the document must be available for inspection.

A risk assessment should be performed in conjunction with system development. A high-level risk assessment should be conducted during the initiation phase of the system life cycle. Additional risks may be identified as systems development progresses through requirement definitions, design, coding, and testing.

The individual risk assessments where required to be done, will consist of the following processes:

Risk Assessments

a. Threat Determination

b. Vulnerability Identification

c. Estimation of Potential Losses

d. Safeguard Analysis

e. Cost-Benefit Analysis

f. Final Report

g. Summary Risk Assessment File

Safeguard Selection and Implementation

a. Management Decisions

b. Implementation

1. Risk Assessment Process

The objective of a formal risk assessment is to determine the current security status of a sensitive application system, information system, information technology facility, or LANs/WANs. First, specific threats and vulnerabilities are identified and analyzed. Next, potential safeguards are evaluated to select those that are most cost-effective in addressing the threats and eliminating or reducing the vulnerabilities to an acceptable level. Lastly, a final report is prepared which summarizes the findings and presents a set of recommendations that are ranked by priority. The final report of several risk assessments across the organization may become the basis for a Summary Risk Assessment File, leading to policy development/change.

a. Threat Determination

Threat determination requires the identification and assessment of potential threats to a sensitive application system, information system, information technology facility, or LAN. Potential threats include both natural disasters and people who can disrupt operations or time-dependent services, or can cause loss of physical assets, loss of systems integrity, or harm to the business of the organization. Each risk assessment is to result in a summary list of threats for every aspect of the sensitive application system, information system, information technology facility, or LAN.

b. Vulnerability Identification

Vulnerability identification involves the determination of weaknesses or flaws that exist in a sensitive application system, information system, information technology facility, or LAN, and that could allow a threat to affect its security. Vulnerability identification should be performed on new, existing, and recently modified sensitive application systems, information system, information technology facilities, and LANs.

A summary list of vulnerabilities should be prepared for each sensitive application system, information system, information technology facility, and LAN being analyzed. The following areas of vulnerability might be addressed:

1. Opportunity for entering erroneous or falsified input data.
2. Opportunity for unauthorized access.
3. Ineffective administrative controls.
4. Ineffective application program controls.

c. Estimation of Potential Losses

After threats and vulnerabilities have been determined, the dollar value of potential losses, including both one-time and recurring costs, must be quantified.

In the case of loss of data or program files, for example, the loss potential is the cost to reconstruct the files, either from backup copies or source documents, and possibly the cost of delayed processing to the user. However, when time losses are more critical than dollar losses, then time loss, rather than cost, becomes the appropriate measure.

d. Safeguard Analysis

The next step includes the identification and assessment of possible safeguard measures and their related costs. The safeguards identified must fulfill the minimum-security safeguard requirements outlined in Chapter III Paragraph C, “Matrix of Minimum Security Safeguards").

e. Cost-Benefit Analysis

During this step, a priority is assigned to each threat or vulnerability (e.g., essential, important, marginal). The costs of the possible safeguards are then compared to the estimated costs of losses which could be expected if the safeguards are not implemented. Situations in which the cost of a safeguard is determined to outweigh the benefit of its implementation should be documented.

f. Final Report

When the risk assessment is complete, a final report is prepared. The report should include the following:

1. List of threats and vulnerabilities.

2. List of safeguards, including alternatives whenever there is more than one possible safeguard.

3. Cost-benefit analysis for each threat or vulnerability and the potential safeguard measures.

4. Recommended safeguards, based on the cost-benefit analysis.

5. Signature(s) by appropriate official(s).

A copy of the Risk Assessment must be supplied to the Headquarters ISM.

2. Safeguard Selection and Implementation

a. Management Decisions

Based on the risk assessment report, and with the assistance of the ISSO, SISSO, System Managers, and LAN Managers, (as appropriate) the managers of sensitive application systems should select specific security safeguards that permit the greatest reduction in exposure for the least total cost. As part of this process, managers should identify any safeguards that can protect multiple application systems, information systems, information technology facilities and LANs. They should also identify any actual or potential safeguards in a system that may affect another system negatively.

If management decides that the benefits of a security safeguard do not justify the costs, the SISSO must document the decision not to meet a security requirement. In such situations, the responsible management official assumes the risk for the decision, and the documentation must be available for inspection.

OSM organizations may request authorizations from the Deputy Chief Information Officer for Information Resources Management (DCIO) to waive or to delay compliance with Federal security requirements or standards. The DCIO will determine whether the waiver request should be forwarded to the appropriate government official for approval.

b. Implementation

System Managers, Facilities Managers, LAN Managers, and the managers of sensitive application systems, in coordination with the SISSO, must determine a schedule for implementing selected safeguards. The schedule must consider mission priorities and budget constraints, as well as the urgency associated with safeguarding sensitive systems.

The ISSO will also develop a plan for reviewing the implementation of safeguards. The DCIO will review and approve all implementation plans for accuracy and adequacy.

Whenever the safeguards that apply to a system of records subject to the Privacy Act are significantly altered as the result of a risk assessment, the organization's Privacy Act Officer must be notified.

Chapter V. Security Program Plan

A. Overview

This chapter presents the policy for developing security plans. The Computer Security Act of 1987 requires the development of a security plan for each computer system that contains sensitive information. The security plan assists OSM in addressing the protection of the general support system, LAN/WAN and the current major applications. This chapter presents policy for determining the sensitivity of information databases and the operational criticality of information application systems. The requirements contained in this chapter apply to all OSM organizations that use information systems and information databases. Organizations should use the guidance presented in this chapter to ensure the security of their information systems.

OSM presumes that all of the data that are collected, maintained, and processed by an organization have some value. However, since neither all data nor all data applications are of equal value or sensitivity to an organization, they need to be categorized and protected differently. Databases and application systems that are categorized with high sensitivity designations require more stringent security safeguards than those with low sensitivity designations do do. Databases and application systems that are categorized at the lowest end of the spectrum usually require only minimum precautions.

1. Data Exchange

Data received from one Bureau, agency, or organization for use by another Bureau, agency, or organization must carry the security level designation assigned by the owner. FPPS and data from individual states are examples of these types of data systems.

2. Integration of Computer Security into System Development Life Cycle

A control process must be established to ensure that appropriate administrative, physical, and technical safeguards are incorporated into all new applications and significant modifications. At a minimum, for each sensitive application, organization management is responsible for:

a. Defining and approving security specifications prior to programming.

b. Conducting and approving design reviews and tests of security features prior to the release of a system.

B. Computer Systems Security Plans

A security plan must include:

1. **System Identification** – Includes the responsible organization, the system name or title, the system category (major application or general support

system), the system operational status, a description of the function and purpose of the system, a description of the system environment, and contact person(s).

2. Sensitivity of Information Handled – Includes applicable laws and regulations, and a description of information sensitivity in terms of type (confidentiality, integrity, availability) and relative importance (high, medium, low) of protection needed.

3. System Security Measures – Includes a risk assessment, applicable guidance, required security control measures, and status (in place, planned, not applicable) for each control measure.

4. Additional Comments – Provides an opportunity for additional comments on system security or perceived needs for guidance or standards.

Note that a single Security Plan may serve a group of applications. Refer to the NIST Special Publication 800-18 as a guide to developing security plans. The System Manager approves the Security Plan. The Security Plan is reviewed and adjusted every three years.

C. Application System Review

The review consists of a technical evaluation of sensitive application to see how well it meets its security requirements.

The Reviewers prepare a report based on the technical evaluation. They then decide on the acceptability of application security safeguards, approve corrective actions, ensuring that corrective actions are implemented, and issue the review statement. While most flaws will not be severe enough to remove an operational system from service, they may require restriction on operation (e.g., procedural security controls).

For new application systems, the review process must begin during the design and development stages. Sensitive application systems must be reviewed at least once every three years. Every sensitive application system must be reviewed if the safeguard requirements outlined in this *Document* change, the system is violated, or the system undergoes a significant modification.

At a minimum, the reviewing official should review the following documents during the review process for a sensitive application:

1. Computer Systems Security Plan
2. Security specifications and test results
3. Contingency Plan
4. Other pertinent documents (e.g., risk assessments, audits, Information Resources Management reviews)

NOTE: The Reviewing Official may be the Application Systems Manager; however, the more sensitive the application, the higher the management level of the reviewing official should be.

When the reviewing official is satisfied that appropriate safeguards are in place for the application system and that the data processed by the application system are or will be secure, the procedure is as follows:

1. The Reviewing Official completes three copies of the "Application System Security Review" (See Chapter V, D, to document the review procedure.)

2. The Application System Manager retains one copy of the security review form and forwards one copy of the form to the organizational Information System Security Officer. The third copy may be retained for central files.

3. Applications that do not meet procedural or substantive security requirements should not pass the review. In such cases, a deferral statement includes a list of deficiencies that must be remedied. The review must be reported as a security weakness under the A-123 reporting process.

C. Application System Security Review

Sample Application System Security Review Statement:

Application System Security Review

I have carefully reviewed the attached computer system security plan together with the findings and recommendations of a documented risk assessment; analysis of threats, vulnerabilities, and safeguards; or security evaluation performed within the past three years. Based on my authority and judgement, and weighing the residual risks against operational requirements, I authorize continued operation of (name of system) application system under the following restrictions:

(Restrictions, if any)

I further authorize initiation of the following corrective actions, to be completed within the next calendar year:

(Corrective actions)

____

(Signature/Title of Reviewing Official)

E. No Pass Review

Sample No Pass Review Statement:

No Pass Review

Based on a review of the attached computer system security plan, requirements set forth in OMB Circular A-130, and the security requirements of (name of system) , this application cannot be passed at this time. The reasons for deferral includes:

[ ] An analysis of threats, vulnerabilities, and safeguards has not been performed within the last three years.

[ ] No documented security specifications exist.

[ ] Documented testing of security specifications has not been performed within the last three years.

[ ] Major vulnerabilities exist (specify) ____________

[ ] Personnel screening has not been performed.

[ ] Security awareness training has not been performed.

[ ] Other (specify) _______________________________________

I authorize initiation of the following corrective actions, to be completed within the next calendar year:

(Corrective Actions)

____

(Signature/Title of Reviewing Official)

F. Application System/Database Security Safeguard Matrix

Explanation: This matrix provides guidance for identifying the minimum required security safeguards for information application systems and databases.
Directions: Locate the security level designation of the application system/database in the left-hand column. An "X" to the right of the security level designation means that the security safeguard listed above is required, and an "O" means that the security safeguard is optional.

	Security Safeguards					
Security Designation	Access Controls	Encryption	Backup Copies	Audit Trails	Periodic Risk Analysis/ Review	Physical security
Sensitive	X	O	X	X	X	X
Non-sensitive	O	O	O	O	O	O

Chapter VI. Contingency Planning

A. Overview

Each OSM organization is responsible for developing and testing a formal contingency plan for each of its major Information Systems, information technology facilities, Local Area Networks (LANs) and its Wide Area Network (WAN). Major information systems are defined as any automated data processing system that meets at least one of the following criteria:

1. A system designated as an OSM Sensitive Automated Information System, i.e. ABACIS, AFBACS, AMLIS, AVS, CPACS, CDR (Coal Data Repository), Electronic Mail, FEEBACS, GIFTS (Grants Information Fund Tracking System), Litigation Tracking System, FPPS, IDEAS, TIPS (Technical Information Processing System), CTS (Correspondence Tracking System), OSMNET (Wide Area Networking System), WATTS/MIPPS (Work Assignment Tracking System/Mine Information Project Planning System), and ARMS (Administrative Records Management System);

2. A system, standalone or one shared on a LAN or WAN, that is used every week by employees within an organizational structure, in carrying out its official functions and duties;

3. A system residing on an OSM LAN which is accessed on a regular basis by OSM employees or contractors;

4. A client/server system residing on NT, Unix, Linux, or Novell accessed by OSM employees or contractors;

5. A system used to deliver dynamic HTML content for access by web browsers;

6. A system hosting or accessing data that is considered proprietary, e.g., coal operator data, sensitive data, or data subject to the Privacy Act.

Contingency plans are also required for stand-alone microcomputers (since microcomputers are technically considered to be facilities), but a single plan for multiple microcomputers may be appropriate.

The plan must detail how the organization would continue its mission and provide continuity of data processing if service, use, or access was disrupted for an extended period of time; for example, if a power outage occurred following a natural disaster. The plan **must** be coordinated and integrated with the contingency plans of other programs (e.g., internal controls, and emergency preparedness), as appropriate. The plan must be documented in the organization's Information Systems Security Program (ISSP).

This chapter describes the contingency planning process at the organizational level. The process includes development, maintenance, testing, and implementation. The information in this chapter applies to all OSM organizations that use information databases, information technology facilities and LANs or stand-alone microcomputers, including those provided by contractors. If an organization contracts for automated data processing (ADP) services that are critical to the performance of its mission, the contract must document the need for contingency plans and require the contractor to demonstrate the ability to provide continuity of data processing in the event of a disaster.

This plan requires a risk assessment to identify potential threats to its systems and networks. (See Chapter IV, "Risk Management.") In conjunction with this risk assessment, each organization can determine the extent to which a Computer Security Incident Response Capability (CSIRC) would provide a cost-effective safeguard.

B. Introduction to the Contingency Planning Process

A contingency plan must be developed for each information technology facility, LAN and WAN, or stand-alone microcomputer that processes applications critical to the performance of the organizational mission. However, there are major differences in the level of detail required for different size and types of systems. Therefore, following discussion of those aspects of contingency planning common to information technology Facilities/LANs and stand-alone microcomputers, this chapter treats these two contingency planning processes separately, with the major emphasis on contingency planning for information technology facilities, LANs, including network contingency planning.

Each OSM organization should make every effort to administer the contingency planning process in an integrated manner across all its systems, facilities, and networks, in order to allocate resources equitably and discover and address points of interface. Moreover, contingency planning for entire service and delivery systems, such as electricity and telephone service, must be considered. The following list includes key steps in the contingency planning process that are common to both LANs and stand-alone microcomputer. (See also Chapter X “Desktop, Software and Systems.”):

1. Identify critical applications.

2. Rank applications according to priority for recovery.

3. Define the maximum permissible outage (i.e., disruption of service, use, or access) for each application, in conjunction with the program manager.

4. Back up critical applications, data, operating software, and databases regularly.

5. Explore alternate IS processing sites within or outside the organization.

6. Select and commit to an alternate site, based on a mutual aid, building, leasing, or contracting agreement.

7. Develop alternate site operating procedures.

8. Arrange for delivery of backup data and software from an off-site security storage facility.

9. Implement tests at the alternate site using backup data and software from the off-site security storage facility.

10. Continue to test regularly.

11. Update the contingency plan based on test results.

C. Contingency Planning Process for IT Facilities/LANs

1. Elements of the Plan

The following elements should be included in the contingency plans for information technology facilities, LANs and WANs:

a. Alternate Site

The contingency plan should provide for an alternate site to perform the data processing functions of the organization if a disaster seriously disrupts the services of a principal information technology facility or LAN. Furthermore, there should be reasonable assurance that the alternate site will be available in the event of a disaster; and that it will be available for testing the contingency plan.

The first choice for an alternate site is within the organization. For example, an organization which processes data within a distributed processing environment or uses multi-site systems architecture could design its contingency plan so that each site serves as a backup to others. This strategy requires the ability to divert inputs to and outputs from a disabled site, and requires excess processing capacity to handle increased workloads on a temporary basis.

If alternative sites do not exist internally, then the organization should consider fully redundant sites, mutual aid agreements, cold sites, or hot sites.

Fully redundant sites are usually not a viable alternative. Since they must be built to the exact specifications of the primary site and located elsewhere, they will generally be costly and impractical.

Mutual-aid agreements (e.g., Inter-Agency agreements) with other organizations to use their data processing resources can work effectively if each involved organization commits to increasing its data processing capacity.

Cold sites are shells that must be equipped to operate as alternate sites. Since they require a two-to-three week delay while the necessary equipment is installed, cold sites may not be an acceptable alternative for an organization that depends on online data processing; however, they could be an acceptable alternative for an organization that only requires batch processing.

Hot sites are fully equipped information technology facilities that include computers, support systems, and telecommunications capability. They are available nationwide for lease. The leasing fee entitles the user to access to the facility when needed. Additional user fees are usually charged for using the site for testing or during an actual contingency situation. Hot sites are usually the most expensive alternative following fully redundant sites, and availability is on a first-come first-served basis.

b. Hardware

Given the rapidity of technological change, the computer industry is often concerned with upward hardware compatibility. However, in a disaster recovery situation, downward compatibility may become the primary concern; e.g., a critical tape must load properly on the backup hardware system. If the alternate site is a mirror image of the principal site, as is usually the case in a multi-site organization, hardware compatibility is not an issue. In any other approach to contingency planning for large information technology facilities and LANs, however, hardware requirements must be defined to ensure compatibility with the principal site and sufficient capacity to run critical data until recovery is completed.

Hardware includes both computers and peripheral devices. If an online application is deemed critical, telecommunications equipment is also included. If the organization has decided on a cold site, the logistics of ordering and installing the hardware must be addressed. If a hot site is selected, the Statement of Work that is prepared to contract for the service must specify the compatibility and capacity requirements of the necessary hardware.

c. Software and Data

Software and data that are critical to the organization's mission must be backed up frequently and maintained at least one mile away from the information technology facility/LAN. Critical software and data include current operating system software, critical applications software, and critical databases.

The contingency plan must describe the critical data, specify how frequently the data backed up, and detail the method of delivery to the off-site security storage facility location. The plan must also specify how the backup data will be delivered from the off-site security storage facility to the Off-site Computer Facility.

d. Personnel

The contingency plan must specifically identify the personnel designated to run the Off-site Computer Facility until recovery is completed at the principal information technology Facility/LAN. This position requires a special commitment, as the Off-site Computer Facility is likely to be located a significant distance from the principal information technology Facility/LAN.

The plan must also address travel authorization, per diem authorization, lodging, and other administrative requirements to move personnel from their usual work locations to the off-site computer facilities. Pre-cleared blanket authorizations may be necessary to move personnel to the off-site computer facilities quickly.

e. Operating Procedures

Operating procedures are specific to the off-site computer facilities. They are developed and validated during testing at the Off-site Computer Facility.

f. Recovery

Recovery from a disaster is complete when the principal information technology Facility/LAN is restored to its original condition and is once again capable of full operation. The recovery process starts with an assessment of damage to specific equipment, including all of the information required to identify and reorder the equipment.

Accurate inventories and floor plans are invaluable aids in the recovery process. Copies of these items should be a part of the contingency plan and should be maintained off-site. To strengthen the contingency plan, it is advisable to work closely with the Contract Officer to clear procurement paperwork for hardware, facilities, and LANs prior to actual need.

Once the LAN has been physically restored, the final step to return to full operation involves transporting the critical operating software, applications data, and personnel from the off-site computer facilities back to the principal IT Facility/LAN.

2. Testing the Plan

One appropriate strategy for testing the contingency plan is to test each critical application of the information technology Facility/LAN individually. In this scenario, the software used to run each application is taken to the Off-site Computer Facility to ensure that it runs properly and to develop and validate its operating procedures. After all critical applications have been run separately, the final test consists of running all of them together at the test site. The results of the final test are then used to complete the contingency plan. After it is completed, the plan must still be tested periodically and updated to accommodate any changes, including any updated versions of the software or critical data.

3. Implementation

The final step in the contingency planning process is determining how to implement the plan in the event of a disaster. This step is vital to overcome any confusion or disorganization that may arise during an emergency. It is especially important for personnel with specific responsibilities in the recovery operation to practice their roles in a test situation.

One approach for implementing the plan is to establish a command center. A command center is an office located outside the information technology Facility/LAN which could be occupied immediately and serve as a headquarters for the disaster recovery team. A copy of the contingency plan should be maintained at the command center.

Users must also be notified when the contingency plan goes into effect. At that time, they should begin to operate under emergency processing procedures and alternate means of handling system input and output, based on the shifting of workloads to the off-site computer facility. The procedures developed for implementing the organization's contingency plan must be documented within the plan, and all users should have copies of the plan or be thoroughly briefed on pertinent aspects of the plan.

D. Contingency Planning Process for Stand-Alone Microcomputers

A single contingency plan may serve multiple microcomputers.

In contrast to the costs associated with contingency planning for large information technology LANs based on minicomputers, LANs, and WANs, the costs associated with contingency planning for stand-alone microcomputers are minimal. Therefore, although it needs to be addressed in the contingency plan, hardware replacement is not the main concern in the contingency planning process for these facilities.

The main concerns of the contingency planning process for stand-alone microcomputers are data and software backup, with particular emphasis on customized software that is not available from a retail computer store. The cost to replace customized software may exceed the total cost to replace the hardware.

Chapter VII. Personnel Security/Suitability and Training

A. Overview

This chapter discusses the Bureau's Personnel Security/Suitability Program and how it applies to the OSM Information Systems (IS) Security Program. It sets forth OSM's policy for assigning position risk designations by simplifying and adapting to the needs of the Office of Surface Mining, Reclamation and Enforcement (OSM) the guidance in 5 CFR 731 and 732, and equating those designations to the appropriate background investigation.

This chapter also outlines training requirements. Both OMB Circular A-130 and the Computer Security Act of 1987 require OSM to establish and maintain automated system security training programs. OSM IRM policy directs all OSM organizations to provide microcomputer Security training to all personnel who are involved in the use or management of microcomputers.

It is important to note that the information in this chapter applies to all OSM and contractor personnel. These personnel are defined as:

1. **Consultant/Contractor.**

   An individual performing a service under an agreement or contract to the OSM.

2. **Computer/ADP positions**.

   OMB Circular A-130, Appendix III identifies these as positions involved in the design, development, operation, or maintenance of sensitive applications as well as those having access to sensitive data. These include all positions classified in the GS-334 and GS-335 series as well as positions classified in other series where the majority of time is spent planning, designing, programming, operating or using computer systems, and similar contractor positions. This, however, would NOT include data entry or the collection of data using a computer, nor the development of specifications for what a program should do which are handed off to a computer specialist. Computer related designations would be as follows:

   a. High Risk positions would be the senior management official for OSM computer operations that would be the Chief, ISM.

   b. Moderate Risk positions would be a management or program official which has over-site or responsibility for a major portion of the overall OSM computer system. (LAN Administrators for the Regions, and Branch Chief or Program Managers within ISM.)

   c. Low Risk positions would be those employees who have limited relation to the OSM mission or do not affect the efficiency of services and direction of the OSM.

3. **Employee.**
   Any OSM employee serving under a competitive or excepted appointment.

B. Procedures for Designating and Documenting Position Risk.

The Office of Surface Mining meets the definition of a moderate agency since our activities directly affect the social, political or economic interests of individuals, businesses or organizations in the private sector (the coal mining industry). OSM is also considered a "single-wide" agency since OSM activity is carried out nationally and regionally, with the primary focus extending to the surface mining industry and the states than regulate them. With this determination as a foundation for the overall agency to designate the individual positions within OSM:

a. Management will answer the questions in the attached worksheet and submit along with the position description (PD).

b. Personnel staff will determine position risk designations as follows:

1. If management answers 'Yes' to question 1 (rare in OSM), this would identify the position as a National Security position, not a Public Trust position. Management must then discuss the position with the Security Officer.

2. If management answers 'Yes' to question 2, then the position is placed in the ADP category and management can proceed with the rest of the questions.

3. If management answers 'Yes' for any question 3 through 5, this equates the position to high risk.

4. If management answers Yes for any question 6 through 9, this equates the position to moderate risk

5. If management answers No for all questions 3 through 9, this equates the position to low risk

c. Personnel staff will enter the appropriate position designation on OF-8.

d. Personnel staff/COTR will supply forms so investigations can be initiated within 14 days of placement. (See Chapter VII, Paragraph E)

e. Adjudicate investigation and inform and provide guidance to management on results.

C. Designation Worksheet

Position Risk Designation Worksheet for Federal and Contract Positions:

Position:

Location:

Please review the questions and if you answer yes please explain.

1. Would the incumbent of this position have access to classified material or sensitive, restricted facilities, with national security impact? Most positions in OSM do not.

Yes No

2. Is this position a computer specialist?

Yes No

3. Would the incumbent of this position make or implement policy that could provide the potential to exceptionally seriously impact the operation of OSM or the mission of OSM?

Yes No

4. Is the incumbent in a higher-level management position that could provide the potential to exceptionally seriously impact the operation of OSM or the mission of OSM?

Yes No

5. Is the incumbent an independent spokesperson or assigned to a non-management position with authority for independent action that could provide the potential to exceptionally seriously impact the operation of OSM or the mission of OSM?

Yes No

6. Would the incumbent be in a position to assist in the development and implementation of policy that would provide the potential for moderate to serious impact on the agency or on its program mission and its ability to serve its customer?

Yes No

7. Is the position in a mid-level management position that would provide the potential for moderate to serious impact on the agency or on its program mission and its ability to serve its customer?

Yes No

8. Is the incumbent an independent spokesperson or assigned to a non-management that would provide the potential for moderate to serious impact on the agency or on its program mission and its ability to serve its customer?

Yes No

9. Is the incumbent in a position that delivers independent services to the public, which if services are not met could hurt the public confidence and trust in the agency?

Yes No

Signature of Supervisor and Date

_______________________________________ ______________________________

D. Investigations.

1. Based on the position risk designation the employee will be subject to one of the following back ground investigations:

a. National Agency Check and Inquires (NACI) consists of written inquiries and record searches covering specific areas of an individual's background during the past 5 years.

b. National Agency Check and Inquires with Credit (NACIC) is the same as the NACI with a credit search.

c. Background Investigation (BI) consists of credit check, employment, residences, law enforcement agency checks, personal interviews with the subject and other sources, written inquiries covering specific areas of the subject's background during the most recent 5 years.

2. National Security Position.
Designation of a position at a national security sensitivity level based on the degree of damage that an individual, by virtue of the occupancy of the position, could do to national security. Designations are assigned to assure appropriate screening under EO 10450.

3. Public Trust Positions are those which have the potential for action or inaction by their incumbents to affect the integrity, or efficiency, effectiveness of assigned Government activities. These actions could diminish public confidence whether or not actual damage occurs. Such activities include law enforcement, public safety and health, collection of revenue, and regulation of business, industry, or finance. Most of the OSM's positions fall into this category. Public Trust positions are designated as **Low Risk (LR), Moderate Risk (MR) and High Risk (HR) as follows:**

a. High Risk Positions. Those Public Trust positions that have the potential for exceptionally serious impact involving duties especially critical to the agency or a program mission with broad scope of policy or program authority such as:

1. Policy development and implementation directly related to the direction of the agency. (E.g. Director and Assistant Directors, and Regional Directors.)

2. High level management (Director OSM, Regional Directors.)

3. Independent spokespersons or non-management positions with authority for independent action related directly to the mission/direction of the OSM. (Special Assistant to the Director.)

a. Moderate Risk Positions. Those Public Trust positions that have the potential for serious impact involving duties of a considerable importance to the agency or program mission with significant program responsibilities and delivery of customer service to the public such as:

1. Assistants to policy development and implementation midlevel management assignments

2. Non-management positions with authority for independent or semi-independent action.

3. Delivery of service positions that demand public confidence or trust.

b. Low Risk Positions.
Those positions with less potential for agency impact than those identified as High Risk or Moderate Risk.

E. Investigation Requirements with Costs and Forms

Suitability Investigations*

Position Sensitivity Designation Level**	Security Forms	Required Investigation	Cost (FY 00)	Required Reinvestigation	Cost
Low Risk***	SF-85 & SF-87	NACI	$77	None	N/A
Moderate Risk	SF-85P & SF-87	NACIC	$87	None	N/A
High Risk	SF-85P & Sf-87	BI	$2,695	None	N/A

*Investigations shall not be duplicated when a previous investigation meets the scope and standard for the risk level of the position and the employee does not have a break-in-service of more than 24 months.
**Movement from risk positions to national security positions requires investigation to be upgraded or updated to meet the standard of the national security position.

***Employees appointed for 180 days or less do not need an investigation.

National Security Investigations*

Position Sensitivity Designation Level	**Access Level**	**Security Forms**	**Required Investigation**	**Cost (FY 00)**	**Required Reinvestigation**	**Cost (FY 00)**
Non-Critical Sensitive	Secret	SF-86 & FD-258 – Contractor SF-87 – Federal	NACLC - Contractor ANACI – Federal	$l72 $187	NACLC every 10 yr.	$172
Critical Sensitive	Top Secret	DI-1912, SF-86, FD-258 - Contractor, SF-87 – Federal	SSBI	$2,995	SSBI-PR every 5 yr.	$1,550

*Investigations shall not be duplicated when a previous investigation meets the scope and standard for the sensitivity level of the position and the employee does not have a break-in-service of more than 24 months.

F. IS Training and Orientation Requirements

The Information Systems Management Division will provide training oversight in security training, and Agency reporting.

1. Five general subject areas should be addressed by the training:

   a. Basic Computer Security.

   b. Security Planning and Management.

   c. Computer Security Policy and Procedures.

   d. Contingency Planning.

   e. System Life Cycle Management. Discusses the ways in which security is addressed during each phase of the system life cycle.

2. Target groups for training, plus contractors, may fit into any one of the groups. These groups are as follows:

   a. Executives or senior managers

   b. Program Managers

   c. ISSO and SISSO

   d. LAN Managers, Application Systems Managers, System Managers, and Database Managers

   e. Users, any employees who have access to an OSM computer system. All users of automated information technology must be provided with some kind of general ISS awareness training, whether they use computers on a full or part-time basis to perform their jobs.

3. There are four general levels of training appropriate for different target audiences. The depth of coverage depends on the sensitivity of the information and/or criticality of the systems to which the employee has access, and the employee's responsibility and authority with respect to the information or system.

   a. Awareness level training. Creates sensitivity to threats, vulnerabilities, and the need to protect data and data processing activities.

   b. Policy level training. Provides the ability to understand computer security principles so executives can make informed decisions about computer and information security programs.

   c. Implementation level training. Provides the ability to recognize and assess the threats and vulnerabilities to automated information resources so that the responsible managers can set security requirements which implement Agency security policies.

d. Performance level training. Provides employees with skill to design, execute, or evaluate Agency computer security policies and practices so that employees will be able to apply security concepts while performing tasks that relate to their duties and positions.

IS Training and Orientation Requirements below, adapted from the NIST Training Matrix, provides an overview of the content and appropriate training level for each of the target populations. Subject areas, target populations, and training levels are described in detail following the chart:

	TRAINING AREA				
AUDIENCE CATEGORY	Computer Security Basics	Security Planning & Management	Computer Security Policy & Procedures	Contingency Planning	Systems Life Cycle Management
Executives	Awareness	Policy	Awareness	Awareness	Awareness
Program Managers	Awareness	Implementation	Implementation	Performance	Performance
ISSO, SISSO	Awareness	Performance	Performance	Performance	Performance
LAN, Application System, System, and Database Managers	Awareness	Performance	Performance	Performance	Performance
Users	Awareness	Awareness	Performance	Performance	Awareness

4. Training is an ongoing process and, at a minimum, should be provided whenever there is a significant change in the Agency's information security environment or procedures, or when an employee enters a new position that deals with sensitive information.

All Site ISSO's should receive advanced formal computer training. User training should include security awareness as part of their existing computer training, management courses, and employee orientation. Modes of delivery outside the classroom are acceptable; e.g., computer assisted training, videotapes, workbooks, job aids, and desk guides.

5. Computer security refresher training should be provided annually or as frequently as determined necessary by the Agency, based on the sensitivity of the information that the employee uses or processes.

Chapter VIII. IT Facilities

A. Overview

In accordance with the OSM Information Systems Security Program, all OSM organizations that operate Information Technology (IT) facilities must implement physical security and operating safeguards to protect these assets from unauthorized or fraudulent use, manipulation, or destruction. This chapter presents policies and guidelines for protecting computer facilities and operating systems at the organizational level. The goal is to protect and preserve information, human assets, physical assets, and operating systems by reducing their exposure to vulnerabilities that can disrupt or curtail information systems operations.

The Bureau's information technology facilities are categorized as follows:

1. Government-owned and Government-operated,
2. Government-owned and contractor-operated, and
3. Contractor-owned and contractor-operated.

The policies and guidelines presented in this chapter apply to information technology facilities that house information technology equipment. These policies and guidelines also apply to Local Area Networks (LANs) and to the Wide Area Network (WAN), since the various components of LANs are housed in information technology facilities.

Although stand-alone microcomputers are technically considered to be information technology facilities, they are excluded from the policies and guidelines presented in this chapter, except where specifically referenced, because many of the safeguards discussed in this chapter are not applicable.

B. Physical Security

1. Introduction

In accordance with the OSM Information Systems Security Program, all OSM organizations must implement physical security safeguards to protect the Bureau's information technology resources. These safeguards must be applied in all administrative, physical, and technical areas and can include the use of locks, guards, administrative controls, and measures to protect against damage from intentional acts, accidents, fires, and environmental hazards such as floods, hurricanes, and earthquakes. The minimum safeguards for all information technology facilities are outlined in Chapter III, C, "Matrix of Minimum Security Safeguards." Facilities Management must also ensure that their facilities fully comply with the physical security requirements as defined in NIST Handbook 800-18 and in DOI 444 DM 1, “Physical Protection and Building Security.”

The Minimum Security Safeguards reflect the minimum security requirements that must be implemented until a formal risk assessment of an information technology facility has been conducted. Based on the results of the risk assessment, additional safeguards may be added. If the risk assessment shows noncompliance with security requirements, the reasons why the security requirements cannot be met must be documented, and the documentation must be available for inspection. If an organization cannot implement a Federal security requirement or standard, a waiver request may be submitted to the Deputy Chief Information Officer (DCIO). The DCIO will determine whether the waiver request should be forwarded to the appropriate government official for approval.

Before selecting and implementing safeguards to protect the physical security of information technology facilities, the IT Facility Manager should identify the various components of the information technology facility that require protection. These components may include:

a. Computer room

b. Data control and conversation area

c. Programmer's area

d. Terminal/remote entry

e. Communications equipment area

f. Data file storage area

g. Forms storage area

h. Supplies storage area

i. Maintenance/workshop area

j. Support equipment area

k. Telephone closet

l. Power supply area (including transformer vaults and power panels)

m. General office area (where sensitive data is handled)

The selected safeguards should include, but not be limited to, access control, protection of sensitive materials, IS facility construction, and fire safety.

2. Access Control

The IT Facility Manager must establish physical and administrative controls to prevent unauthorized entry into operations, data storage, library, and other support areas. The following actions should be taken in establishing these controls:

a. Physical Controls

Equip all doors in all areas containing information technology equipment with mechanical or electronic locking mechanisms. Emergency and "Exit Only" doors should be equipped with hardware which permits immediate egress in the event of an emergency.

b. Administrative Controls

Develop and implement administrative procedures for limiting IT facility access to authorized personnel only. To achieve this objective, management should:

1. Prepare and maintain access authorization lists.

2. Discourage the presence of visitors. (When a visit is necessary, require an escort at all times).

3. Maintain logs to record the entry and departure of all individuals, other than normally authorized personnel.

4. Coordinate with the building manager to limit the presence of cleaning and maintenance personnel to the period when regular employees are on duty.

5. Establish procedures to record and report occurrences of non-routine user/operator activity, such as:

   a. Terminals left unsecured after-hours.

   b. Doors to information technology facilities, remote job entry facilities, terminal rooms, library, or media storage areas left unlocked after-hours.

6. Where appropriate post "For Authorized Personnel Only" signs where sensitive data are used or stored.

3. Protection of Sensitive Materials

All OSM organizations should establish procedures to control the handling, distribution, storage, disposition, and destruction of materials that contain sensitive data. The Facility Manager should establish physical and administrative controls to prevent unauthorized entry into operations, data storage, library, and other support areas. The following actions should be taken in establishing these controls:

a. Physical Controls

Ensure that all sensitive materials, such as data printouts and other hard copy materials, software documentation, operating manuals, and handbooks, are labeled as sensitive and stored in a secure location when not in use, preferably in a lockable filing cabinet or desk.

b. Administrative Controls

1. Establish procedures to prevent erroneous or unauthorized transfer of sensitive materials.

2. Ensure that storage media containing sensitive data are labeled.

3. Ensure that the Records Liaison Officer maintains a file and disposition plan for all data in the information technology facility, in consultation with the organization's records management officer. The National Archives and Records Administration (NARA) provides general guidelines for the disposition of electronic records. (See 36 CFR 1234, Electronic Records Management)

4. Dispose of all retired, discarded, or unneeded sensitive data in a manner that will prevent unauthorized persons from making use of it.

a. Ensure that all sensitive data are erased from storage media prior to repair or before release as work tapes, disks, or memory areas (degaussing).

b. Ensure the secure destruction of all sensitive hard copy documents when they are no longer needed.

5. Protect sensitive data during an external evaluation.

4. Facility Construction

The Facility Manager and SISSO must review the construction plans for all new information technology facilities, and for modifications to existing information technology facilities, to determine the most cost-effective method for securing the facilities. The potential vulnerability of the facility to penetration by outside forces, the sensitivity of the data to be processed, and the value of the equipment to be protected should be considered in making this determination.

Minimum protection must be provided for all new information technology facilities and modifications to existing IS facilities using the following guidelines:

a. Walls should be constructed of materials that offer resistance to forced entry and have a fire rating of at least one hour. (Refer to GSA FPMR Subpart 101.36.7 and the Bureau of Commerce RP-1, Standard Practice for the Fire Protection of Essential Electronic Equipment Operations.)

b. All facility doors should be constructed of materials that are comparable to the facility walls in strength and fire rating.

c. The most desirable location in which to house information technology equipment is an interior room, above the first floor, having four solidly constructed walls that extend from the true floor to the true ceiling. Location and construction are particularly important if the information technology equipment will not be attended on a 24-hour basis. Attended information technology equipment requires only a minimum level of protection, since resident personnel easily detect unauthorized access.

d. Basement, first and second floor windows, and windows accessible from adjacent structures should be secured when the facility is unattended. The replacement of glass windows with plastic windows should be considered. If the information technology facility is a potential target for vandalism, windows should be barred, screened, or opaque.

5. Fire Safety

SISSO must ensure that appropriate safeguards are implemented to prevent, detect, and/or suppress fires and protect IT equipment in the event of a fire. The following safeguards are required to ensure fire safety, and many of them will also reduce vulnerability to other environmental hazards. For further guidance on fire safety, refer to Department of Commerce RP-1, *Standard Practice for the Fire Protection of Essential Electronic Equipment Operations*, the National Fire Protection Association (NFPA) Publication 75-1992, *Protection of Electronic Computer/Data Processing Equipment*, and local ordinances and building codes.

Chapter IX. Integrating Computer Security into the System Life Cycle

Overview

The National Institute of Standards and Technology (NIST) defines the system life cycle as "the period of time beginning when the software product is conceived and ending when the resultant software products are no longer available for use. The [system life cycle] is typically broken into phases, such as requirements, design, programming and testing, installation, and operations and maintenance. Each phase consists of a well-defined set of activities whose products lead to the evolution of the activities and products of each successive phase."

Information security should be integrated into the application system life cycle from its inception for several reasons:

1. **It is less expensive.** To retrofit security is generally more expensive than to integrate it into an application.

2. **It is more effective.** Meaningful security is easier to achieve when security issues are considered as part of a routine development process, and security safeguards are integrated into the system during its design.

3. **It is less obtrusive.** When security safeguards are integral to a system, they are usually easier to use and less visible to the user.

For more in-depth discussion of life cycle issue, see NIST 800-18, Chapter 44.

Chapter X. Desktop, Software and Systems

A. Overview

This chapter presents the Information Systems Security Program (ISSP) policy for protecting microcomputers and microcomputer application systems and data from damage, destruction, or misuse. The term "microcomputers" includes workstations, personal computers (PCs), other desktop computers, laptops, notebooks, palmtops, and other portables, such as personal digital assistants and personal organizers.

The requirements of this chapter apply to all organizations that use microcomputers. Additional requirements apply for microcomputers that:

1. Use software developed by the user
2. Communicate with other microcomputers.

This policy also applies to microcomputers owned by OSM but authorized for work outside the office by OSM employees, and microcomputers owned by OSM employees but used for official work-related purposes.

Protecting and safeguarding microcomputer software and data can be a difficult problem, since microcomputers are generally easy to access. Therefore, subject to Federal regulations and penalties, all Application System Managers, supervisors, and microcomputer users are responsible for taking actions to safeguard and prevent the improper use of, damage to, or destruction of microcomputer data, application systems, and hardware. The extent of these actions should be commensurate with the sensitivity of the data, operational criticality of the application systems, the value of the hardware, and the distribution of functions and authority.

B. Controlling Access to Systems

1. The System Manager controls and limits computer system access to individuals requiring system access in the performance of their official duties. The IT Specialist/System Manager must limit the access of system users to the minimum level necessary to perform their official duties.

2. Supervisors must complete a written access request for each staff member requiring system access.

3. The System Manager must review each request for accuracy and technical anomalies and retain the request in central files.

4. Prior to gaining access to any of OSM's computer systems or networks,

each user must agree, in writing, to abide by all OSM computer security policies, procedures and guidelines. This documentation is maintained at the local level.

5. Program managers will determine who within their organization requires access to computer systems. This determination will be indicated by written request.

6. System Managers, sometimes referred to as System Owners, or the designated individual, will terminate user system access upon notification by the user's.

C. Specific Requirements for Externally-Developed Software

1. Only software authorized for business purposes should be used on Federal computers.

2. The use of software purchased by the Government is governed by the terms and agreements established by the software vendors and the OSM procurement process. Opening shrink-wrap coverings can constitute acceptance of the licensing terms stated by the vendor. Employees and contractors are strictly forbidden to use or copy software in a manner contrary to licensing agreements and OSM procurement policies. Infringement of software copyrights may constitute theft.

3. PC software products may not be copied more than the limit provided by contract (e.g., including an archived copy for backup purposes). Employees or contractors who make additional copies to avoid the cost of acquiring software must be held accountable for their actions.

4. Superseded PC software may be taken home by employees only if to do so is permitted by the site-license agreement and approved by management. Management approval should depend on the employee's need to perform official government work at home.

5. Software packages protected by quantity licenses must be tracked to control the copying and distribution of the proprietary software.

6. Application System Managers should introduce and enforce management guidelines to prevent the introduction of malicious software into the work place. (See Chapter XII, "Malicious Software and Intrusions.") In general, only shrink-wrapped software or certified shareware should be used. Application System Managers must forbid the use of software downloaded from external sources (e.g. Internet and bulletin boards), unless the downloaded software has first been checked and approved.

D. Information System Security Checklist for Microcomputers

Explanation: The following questions highlight the information system security requirements for application systems that run on microcomputers. For each "NO" response, provide a written explanation on additional paper for the Application System Manager's files.

REQUIREMENTS	YES	NO
1. Do you maintain an accurate inventory of hardware and software?		
2. Are reports and diskettes properly stored in a secure location when not in use?		
3. Do you maintain and update a list of authorized users?		
4. Have the authorized users been trained in both the operation and use of the microcomputer, as well as in Automated system security requirements?		
5. Are application system access passwords available only to authorized users?		
6. Are the passwords changed when authorized employees leave OSM?		
7. When changes are introduced (e.g., new applications, personnel turnover, telecommunications), are risks re-examined?		
8. Are data files backed up periodically? If so, note how often.		
9. Are both user and software documentation kept current and safeguarded?		
10. Where authorized, is software backed up and the original stored in a safe place?		
11. Do you re-examine security on a quarterly basis?		
12. Are security devices installed and procedures in place, which lessen the risk of theft or unauthorized access to the microcomputer?		
13. Are surge suppressors installed?		
14. Are needed contingency plans in place for microcomputers?		
15. Are sensitive data stored or processed on the microcomputer? (If the answer is "no", proceed to question 17.)		
16. Have employees in computer-related personnel positions, which involve the use of microcomputers, undergone appropriate background investigations?		
17. Has password protection capability been implemented to protect the application system? To protect data?		
18. Are sensitive data protected from unauthorized viewing or use during transmission and storage?		
19. Are reports and diskettes labeled and controlled?		
20. Are unneeded sensitive reports shredded and unnecessary files written over?		

NOTE: Individuals who conduct information system security reviews may request specific documentation in support of your responses. In addition, the results of completing this checklist should be used to determine if sensitive information is processed and/or a Computer Systems Security Plan needs to be developed (or updated).

______________________________________ ____________________
(Signature of Application System Manager)   (Date)

______________________________________ ____________________
(Signature of Organization Information   (Date)
Systems Security Officer)

Chapter XI. Data Communications, Networks, E-Mail, Servers and WAN

A. Overview

This chapter presents Bureau policy for protecting sensitive data that are transmitted by electronic means. The policy applies to all OSM organizations which use data communications equipment to transmit automated data and to contractors who provide any type of automated data communication service, software, or equipment. It applies to all telecommunications technology, Local Area Networks (LANs) and the Wide Area Network (WAN).

Data communications encompass the methods, mechanisms, and media involved in information transfer. Two methods of electronic computer communications exist: temporary connection of two computers via modems, and permanent or semi-permanent linking of multiple workstations or computers on a network. The distinction between the two methods, however, is blurred because microcomputers equipped with modems are often used to connect to both privately owned and public access network computers.

Modem-to-modem communications typically involve dial-in access via public telephone lines to a mainframe or a network. Networks, on the other hand, rely on dedicated phone lines and switching systems or, in the case of LANs, machine-to-machine cabling. Networks tend to use sophisticated transport mechanisms and error-catching procedures to route and store messages sent to and from authorized users.

B. Policy

Every OSM organization must identify its sensitive electronic data and provide effective and appropriate protection for data to be transmitted electronically. The Site Information Systems Security Officer and telecommunications officials in the organization must:

1. Ensure that appropriate data communication controls and safeguards are operating in support of each application system and/or automated system that uses data communications.

2. Determine the appropriateness and adequacy of these controls and safeguards to the needs and data sensitivity of the application system or information system.

3. Verify that the controls and safeguards actually function as specified.

4. Identify and implement changes to these controls and safeguards, as required by changing needs and technology.

5. Insure users are instructed to scan for viruses whenever introducing

programs or data external to OSM's networks, for example, floppy discs brought in from home, downloading public domain software.

OSM and contractor personnel must comply with security measures in OMB Circular A-130 and the DOI Security Manual 375 DM 19. Those documents include responsibilities that must be followed by all OSM personnel. In addition, OSM and contractor personnel working for OSM while using the Internet:

a. Must not be harassing, libelous or disruptive to others while connected to the Internet. Fraudulent, harassing or obscene messages and/or materials are not to be sent, printed, requested or stored.

b. Must not transmit personal data or unauthorized government-owned data across the Internet.

c. Must not knowingly download to government computers any obscene written material or pornography.

c. Must obey all copyright laws.

e. Must not send hateful, threatening, or harassing messages.

f. Must not deliberately attempt to degrade the performance of an information system (including computers, microcomputers, networks and telephone systems), or to deprive authorized personnel of resources or access to OSM Information Systems.

g. Must use OSM sponsored Internet connections for official OSM business only, except for the DOI policy allowing personal use of the Internet during non-work hours.

Local Area Networks

a. The LAN at each OSM office will be under the control of the local LAN administrator, who will coordinate with other OSM LAN administrators in supporting OSM staff's network needs.

b. LAN Administrators will coordinate and cooperate with the OSM IRM Coordinator at Headquarters to ensure that OSM networks inter-operate properly, and that OSM users will use those networks to exchange data in compatible formats.

c. All communications will be through the office networks, except for those applications that a user needs access to that are only available via dial-up. The System Owner must grant approval for access to such applications.

d. All LAN user accounts will require passwords, and will require a password change every 90 days. Passwords must not be reused, and shall consist of a combination of letters and numbers and will be a minimum of six characters long. Users are responsible for safeguarding their passwords. They will not be printed, stored online, or given to others. **Users are responsible for all transactions made using their passwords.** No User may access the LAN with another User's password or account.

g. Special support software/hardware may be installed on OSM computing systems and networks in order to support usage accounting, security, network management, hardware and software inventory and updating functions, and to provide better support to personnel. Authorized OSM personnel, and it's contractors, may access other data fields when necessary for maintenance and security of information systems. Advanced notification of access will be given, except for cases precluded by security and maintenance emergencies. When performing maintenance, every effort will be made to ensure the privacy of user files. However, if violations of policies are discovered, they will be reported to Management.

h. To ensure security, users will not connect a modem or any other network circuit to any OSM LAN for the purpose of gaining access without the consent of the LAN Administrator.

i. Each User must ensure the security of the OSM LANs and attached computer resources. This duty includes taking reasonable precautions to prevent intruders from accessing the agency's LANs without authorization.

h. Each User must take reasonable precautions to ensure he or she does not introduce viruses into an OSM LAN. **To that end, all material received on floppy disk or other magnetic or optical medium and all material downloaded from the Internet, or from computers or networks that do not belong to OSM, *MUST* be scanned for viruses and other destructive programs before being placed onto the LAN.** Users should understand that their home computers and laptops might contain viruses. All disks transferred from these computers to OSM's network MUST be scanned for viruses.

i. Where available, password encryption utilities should be used to prevent malicious or inadvertent disclosure of passwords and to prevent powerful system passwords and accounts from being compromised when traveling across a network, such as the Wide-Area Network and the Internet.

Electronic Mail

a. OSM's electronic mail system will be under the control of the Network Systems Support (NSS) staff in HQ for maintenance purposes.

b. OSM users are encouraged to establish separate passwords for their email accounts, and will be required to do so in order to access their accounts across the Internet via web browser interface.

c. Each local E-mail installation will have the security level set to high.

d. All attachments to email messages, whether sent or received, will be scanned for viruses, by the user, using the virus scanning software installed in the local office.

e. Users will not allow others to use their accounts, except for proxy access granted to enable sharing of information. Users will not leave their email accounts "up" on their PC when away from their desks.

OSM Wide Area Network (OSMNET)

a. OSMNET is under the control of Network Systems Support (NSS).

b. Host-based security will be the primary method of protecting OSM systems. This methodology will be enhanced by packet filtering and/or 'firewalling' as necessary.

c. No connections of any kind will be made to OSMNET without approval of NSS.

d. The protocol of OSMNET will be the Internet Protocol (IP), with some IPX protocol being routed on tail circuits, as approved by NSS. IPX shall not be routed across DOINET or the Internet.

e. The OSMNET is an open network, with security implemented at the individual node level through packet filtering and/or 'firewalling.'

f. Firewalls will be a function of NSS, and not be undertaken by the local nodes without NSS approval.

g. Any security change at the local node will be supported by a Risk Assessment, and a detailed requirements document.

h. Any dial-in connections to OSMNET must be coordinated with the NSS, and be supported by a brief requirements document.

i. Internet connectivity from OSMNET will be controlled by NSS. Individual Internet connections from local nodes will not be allowed.

j. All change requests for OSMNET will have Management approval before being presented to NSS for consideration, security being a foremost consideration.

Internet

The responsibility for protecting OSM resources on the Internet is the responsibility of the NSS and the program offices that have Internet servers available to the public. This policy also applies to contractors.

A fire wall compromise is potentially disastrous to internal security. For this reason, OSM will, as far as practical, adhere to the following stipulations when configuring and using firewalls:

a. OSM will strictly limit incoming access to OSM data and systems by Internet users.

b. Where servers are accessible to the public, and a firewall is used, the Demilitarized Zone (DMZ) concept will be part of the firewall architecture. This concept is not required where local conditions do not warrant its use. Limit firewall accounts to only those absolutely necessary, such as the administrator.

Note: A DMZ is an area between the trusted, or inside, network and the untrusted world of the Internet. The term refers to a physical and technical placement of firewall devices, routers and computers. The DMZ contains routers, firewall and Web servers and perhaps other computers that the outside world is allowed to see. The firewall is what controls the traffic and allows trusted users into the trusted network. Probes by hackers thus occur in this area and not inside the firewall.

c. Remove compilers, editors and other program development tools from the firewall system(s) that could enable a hacker to install Trojan Horse software or backdoors.

d. Do not run any vulnerable protocols on the firewall.

e. Disable the finger command. The finger command can be used to leak valuable user information.

f. Do not permit loopholes in firewall systems to allow friendly systems or users special entrance access. The firewall should not view any attempt to gain access to the computers behind the firewall as friendly. Modems provide a back door to a secure Internet; therefore, the use of modems for anything other than dialing out is expressly prohibited for any network-connected workstations unless authorized by NSS.

g. Disable any feature of the firewall that is not needed, including other network access, user shells, applications and so forth.

h. Firewalls will employ auditing, reporting and notification techniques to track security incidents, keep logs and warn the appropriate security personnel when violations occur.

i. Proxy services and caching improve security levels and can increase efficiency on the network. Therefore, proxy services shall be used where practical and advisable.

The Computer Security Act of 1987 assigned the National Institute of Standards and Technology (NIST) the responsibility for developing computer security standards and guidelines for unclassified Federal systems, including data communications systems and networks.

C. Sample LAN/WAN Security Plan Checklist

Explanation: This checklist is designed to help IRM management, information technology security officers, and LAN officials review security plans for LANs and WAN. It is keyed to the major elements of the Computer Systems Security Plan (CSSP) format as presented in OMB Bulletin 90-08, "Guidance for Preparation of Security Plans for Federal Computer Systems that Contain Sensitive Information."

Yes/No Questions		Yes	No	N/A
1.	Have Computer Systems Security Plans (CSSPs) been implemented for LANs and WANs designated sensitive?			
2.	Does each CSSP contain the following information?			
	a. Name, category, operational status, description and environment adequately identify systems.			
	b. Each CSSP identifies additional applications and systems covered.			
	c. Information sensitivity is identified by type (confidentiality, integrity, and availability) and relative importance (low, moderate, and high).			
	d. The magnitude of potential harm or loss is identified.			
3.	Does each CSSP indicate whether control measures are in place, planned, or not applicable for:			
	a. Assignment of security responsibility			
	b. Risk assessment (within last five years)			
	c. Personnel screening			
	d. Acquisition specifications			
	e. Security and awareness training			
	f. Operational controls:			
	(1) Physical and environmental protection			
	(2) Production and input/output controls			
	(3) Emergency, backup, and contingency planning			
	(4) Audit and variance detection			
	(5) Hardware and system software maintenance controls			

	(6) Documentation			
	g. Technical controls:			
	(1) User identification and authentication			
	(2) Authorization/access controls			
	(3) Integrity controls			
	(4) Audit trail mechanisms			
	(5) Confidentiality controls			

Chapter XII: Malicious Software and Intrusions

A. Overview

Computer systems and communication networks are subject to a variety of threats, many of which have emerged during the past decade with the enormous growth in the use of microcomputers and Local Area Networks (LANs). These threats fall into two categories: malicious software and intrusions.

Malicious software is the collective name for a class of programs intended to disrupt or harm systems and networks. The most widely known example of malicious software is the computer virus.

Intrusions are penetrations of computer systems and networks by hackers. Hackers may be legitimate users who overstep the bounds of authorized access or outsiders who break into systems for which they have no authorization.

B. Malicious Software

A **Trojan horse** is "a destructive program disguised as a game, a utility, or an application. When run, a Trojan horse does something devious to the computer system while appearing to do something useful."

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

A **worm** is "a program that propagates itself across computers, usually by spawning copies of itself in each computer's memory. A worm might duplicate itself in one computer so often that it causes the computer to crash. Sometimes written in separate 'segments', a worm is introduced surreptitiously into a host system either for 'fun' or with intent to damage or destroy information."

C. Intrusions

A hacker is a person "who secretively invades others' computers, inspecting or tampering with the programs or data stored on them." Hackers use a variety of techniques to gain unauthorized access, including:

1. **Password cracking**, in which the hacker tries easily guessed passwords, or uses a dictionary as a source of guesses for an automated attack.

2. **Exploiting known security weaknesses**, in which the hacker takes advantage of vulnerabilities such as a configuration error that grants file access to all users, or makes use of "trapdoors" originally inserted by system developers for system maintenance.

3. **Network spoofing**, in which the hacker's system impersonates another system when attempting to log on to a network.

D. Safeguards

Sections H through K chart four categories of safeguards against the threats posed by malicious software and intrusions. The categories include technical controls, software management, contingency planning, and system monitoring/intrusion detection. Each of these tables contains examples of safeguards that can be used for computers of all sizes.

E. User Security Awareness Training

Section L charts subjects that can be addressed in elevating user awareness about malicious software and intrusions. Users must understand what is expected of them and what activities are violations of policy, such as loading unapproved software on their microcomputers or using systems and data for which they are not authorized. They must be instructed in how to use the system safeguards that protect systems and data. Adequate user awareness training can go a long way toward preventing the effects of malicious software and hackers.

F. Sign-On Warning

In conjunction with a review of the legal propriety of keystroke monitoring, the Department of Justice (DOJ) has advised the National Institute of Standards and Technology (NIST) that government agencies should warn system users that, by using a system, they are expressly consenting to keystroke monitoring. Provision of written notice in advance to only authorized users is not sufficient. Since it is important that unauthorized intruders be given notice, some form of banner notice at the time of signing on to the system is required.

An agency's banner should give clear and unequivocal notice to intruders that by signing on to the system they are expressly consenting to such monitoring. The banner should also indicate to authorized users that they may be monitored during an effort to monitor an intruder (e.g., if a hacker is downloading a user's file, keystroke monitoring will intercept both the hacker's download command and the authorized user's file). In addition, system administrators may monitor authorized users in the course of routine system maintenance.

DOJ and NIST have provided the following example of an appropriate banner. It is the only official guidance available at the time of publication of this Handbook regarding sign-on warnings:

This system is for the use of authorized users only. Individuals using this computer system without authority, or in excess of their authority, are subject to having all of their activities on this system monitored and recorded by system personnel. In the course of monitoring individuals improperly using this system, or in the course of system maintenance, the activities of authorized users may also be monitored. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence of such monitoring to law enforcement officials.

No specific language is required at this time, and Agencies are encouraged to tailor the banner to their precise needs. For example, the banner might contain a statement concerning the need to protect private data from unauthorized disclosure (e.g., *"The Privacy Act of 1974 states that all private data must be protected from unauthorized disclosure. Anyone reading this data is responsible for the privacy of data displayed on a computer monitor/CRT or printed in a report."*). An agency may also want to consider mentioning the legal penalties to an individual who signs on to a Federal system without authorization.

G. Computer Security Incident Response Capabilities (CSIRC)

Computer systems and communication networks are subject to a variety of sophisticated threats. Malicious software, in particular, is a large and growing threat that can cause enormous harm in a short period of time. Prevention, by the use of anti-virus software must be the main line of defense. When a security incident occurs there is a need to respond quickly with on-call expertise that can control and contain sophisticated intrusions, limit damage, eliminate the problem, and restore normal operations.

Currently most problems of an immediate nature are dealt with by contacting the ISM Headquarters Computer Support Center to discuss the problem with knowledgeable peers. Most problems involving hardware, software and procedures are effectively resolved in making this call for assistance.

A CSIRC is a part of the computer security effort that provides the capability to respond to computer Security threats rapidly and effectively. The FedCIRC provides the means for the Federal agencies, law enforcement, private sector, and academia to work together to handle IT Security incidents, share related information, solve common IT security problems, and plan future IT Infrastructure protection strategies. A CSIRC provides a way for users to report incidents, and it provides personnel and tools for investigating and resolving incidents, and mechanisms for disseminating important incident-related information to management and users. The Department of the Interior currently has a Letter of Agreement with The Federal Computer Incident Response Capability to provide this direct assistance.

1. CSIRC components:

a. The OSM Point of Contact, is the ISSO (202) 208-2910, or page at (202) 319-2013, (CSIRC Coordinator ISM,) is responsible for follow-up reporting and issues clarification.

b. The FedCIRC Management Center POC can be contacted at
(202) 708-7201 (Computer Emergency Response Team).

c. The FedCIRC Operations Center (Carnegie Mellon University Software Engineering Institute) POC can be contacted at (888) 282-0870.

d. Communication is maintained with the FedCERC facilities and the DOI user community.

e. A contact list is used to facilitate rapid communication.

2. Steps to dealing with CSIRC:

a. Contact ISM Headquarters Support Center, if possible, as a first step.

b. Contact other DOI POC for assistance if appropriate.

c. Contact FedCERC facilities at any time if you wish to report, access information or need assistance on a incident response action.

d. Report all IT security incidents to the ISSO.

H. Technical Controls

Password Management	Require effective passwords for all logons.
	Eliminate easily guessed passwords, including all proper names and dictionary words.
	Make password files inaccessible.
	Schedule regular password changes.
	Accept only a limited number of password attempts before disabling an account.
File Access Management	Set default access for all files to owner-only.
	Provide access only to programs and users who require access.
	Provide only read access unless write access is required.
	Review access permissions periodically.
Microcomputer Accessibility	Reduce microcomputer accessibility by: Removing floppy disk drives or using diskless computers. Using commercial software to provide password protection. Using add-on hardware for user authentication.

I. Software Management

System Software	Stay abreast of known operating system vulnerabilities and specific fixes (Service packs and fixes).
	Use current versions of all operating systems.
	Prevent user access to system software and data.
	Identify and eliminate or change any "trapdoors" inserted by system developers.
User Software	Prohibit users from installing software directly.
	Develop a mechanism, such as virus scanning, for validating software (particularly public domain software) before installation.
	Only install software (e.g., compiler or debugger) that is clearly needed on user machines.
	Prohibit users from adding software to LAN software repositories.
	Maintain a database of all installed user software for quick location of suspect software.

J. Contingency Planning

Backups	Write-protect application software diskettes.
	Back up and safe-store application software.
	Restore software only from its original medium, rather than from backup tapes/disks.
	Follow a regular schedule for data backup.
Incident Response	Develop a Computer Security Incident Response Capability (CSIRC). (See Chapter VI, "Contingency Planning.")

K. System Monitoring/Intrusion Detection

Tools	Use virus scanners for routine checks of all microcomputer and LAN software.
	Use system audit tools to monitor accesses to accounts and files.
	Use system sweep programs to checksum files and report differences.
Procedures	Review monitor tool logs regularly.
	Investigate all suspicious activities.
	Enforce sanctions against users who consistently violate security policies.

L. Necessary User Awareness Training

Malicious Software and Intrusions	Methods of operation and transfer of malicious software; nature of intrusions
	Vulnerabilities exploited by malicious software and hackers
	Security and productivity consequences
Safeguards	Security policies and procedures
	Recognition of abnormal system activity
	Role of CSIRC

Chapter XIII. – Access Controls

A. Overview

This chapter establishes policies and procedures designed to safeguard information systems and data by establishing system access controls. All personnel will adhere to the following requirements classified as LAN Administration, Personnel Practices, Access Rights, Custodial, Telecommunication, Evaluation and General.

B. LAN/System Administration Requirements

Administrators will implement technical controls necessary to ensure that the threat to powerful network operating system commands by unauthorized individuals is minimized. Inappropriate control over these commands could allow unauthorized users to gain control over network resources. Examples of these commands in a Novell operating environment include 'Secure Console', 'Lock Console' and 'Rconsole'. The Administrators will ensure that all steps have been taken to minimize the inappropriate use of these commands by unauthorized individuals. The following must be ensured:

1. The user-ID will be unique to each user and will identify the user to the system. The assignment of more than one user or a phantom user to a user-ID is prohibited.

2. Whenever possible, passwords will be user generated under the supervision of access control software. In facilities where access control software is not available, the IT Specialist/System Manager will create and distribute user passwords in a controlled manner, and in such a way that an audit record of password date and time of issuance, receipt, use, change, expiration and termination is maintained.

3. System users will gain access to networks or distributed systems only after entering their unique user-ID and a password.

4. Passwords will be valid for a period of not more than 90 days.

5. System users will not share their system passwords with anyone, even another cleared user.

6. System Administrators must activate the audit trail capabilities provided by the operating system and security software installed on Agency systems.

7. System Administrators will manage the creation, use and deletion of user IDs and password to prevent unauthorized access to the system. This process will ensure that employee terminations, transfers, or re-assignments of

responsibilities result in a subsequent assessment of the need for user accounts and associated user rights to files and systems. This process will be carried out in a uniform and consistent manner throughout OSM, and will be achieved in concert with standard operating procedures of the Office of Personnel for Federal employees and individual Contracting Officer Technical Representatives for contract employees.

8. The SISSO must ensure all system users are aware of the private nature of their passwords. Users must inform the Administrator if they suspect their password has been compromised.

9. ISSO and System Managers will ensure that Administrators log onto information systems under specific user ID's designated for system administration purposes.

10. Password file maintenance will be restricted to the LAN Managers and System Administrators, and passwords will be screen-suppressed during logon and re-authentication.

11. Users will be required to use passwords randomly selected and consisting of a combination of at least six alpha, numeric or special characters that cannot be traced back to the user (recognizable words, phrases, or dates must not be used).

12. When the password expires, the operating system or security software must prompt the user to change passwords.

13 An audit trail will be implemented and viewed periodically and will record at least the following events and any other events deemed appropriate by the Responsible Official:

a. Multiple logon failures;

b. Logons during non-business hours;

c. Addition, deletion, or modification of user or program access privileges; and

d. Changes in file access restrictions.

14. System Administrator must archive the audit trail to a file with the most stringent access restrictions available. Audit trails containing financial information and transactions must be retained for a period of two years. Audit trails containing information not related to financial information and transactions must be retained for an appropriate time period.

15. The System Administrator will not maintain permanent user-IDs and

passwords on computer systems for visitors, vendor service personnel, training, or demonstrations.

16. The System Administrator will delete all default user-IDs and passwords supplied by the vendor during system manufacture and installation once installation is complete.

17. The System Administrator must cause all system users to change their passwords under the following conditions: at least every 90 days (30 days for dial-in access); immediately following any suspected compromise; and whenever there are changes in personnel with system security authority.

18. The System Administrator must immediately delete user-IDs and passwords whenever the Supervisor determines that the user no longer requires system access. (See Chapter I Paragraph E, 13e)

19. Use of information systems equipment owned or operated by the Agency for purposes other than authorized U.S. Government use is prohibited.

20. Logged on workstations are not left unattended unless locked or password protected. However, employees will not engage or set Basic Input Output System (BIOS) password access controls on individual PCs.

21. After-Hour System Operation

a. The Site ISSO and System Managers must ensure appropriate after-hour restrictions are developed and implemented for each system under their purview.

b. The System Manager must ensure all system logs in effect during normal operations are also activated during after-hour operations.

22. Protection of Media and Output - The System Manager must store back-up copies of operating system and application software, in an authorized off-site locked area or approved security container.

C. Personnel Practices Requirements

Only individuals who meet the requirements for sensitive systems and related automated data processing positions (those with proper clearances) will be users with special access privileges.

D. Access Rights Requirements

Program Managers are responsible for ensuring separation of duties and implementing controls to prevent fraud, waste and abuse.

1. Accordingly, the System Manager, or System Owner as appropriate, must structure user access privileges to reflect the separation of key duties implemented for functions supported by the application. All user access privileges must be consistent with the separation of duties established for manual processes and be reviewed on an annual basis.

2. The System Manager, or System Owner as appropriate, must revoke the user access privileges of personnel no longer requiring system access or personnel that have severed their relationship with the Agency. Such revocation must take place immediately upon the employee's status change or departure.

3. The System Manager, or System Owner as appropriate, must implement all application controls to ensure users are assigned access rights and privileges consistent with their functional responsibilities and authorities. Access rights and privileges must be based on need-to-know, separation of duties, and management authorization. This will include assurances that public users do not have inappropriate access to computer resources. It must also ensure that only authorized users have 'root' access.

4. The System Administrator must ensure necessary security controls are implemented to prevent unauthorized access to OSM systems. The System Administrator will ensure that the following restrictions are enforced:

a. The LAN, or host computer systems, disconnects a logged on client workstation or microcomputer from the system after a predetermined period of inactivity.

b. Limit unsuccessful logon attempts from any user account to three. After three unsuccessful logon attempts, the system will automatically lock out the user account. Only the System Administrator will be given the capability to reset a user account after lockout.

c. Any systems that cannot be set to three unsuccessful login attempts will be set to the minimum possible.

d. System Manager, or System Owner as appropriate, will formally assign responsibility for approving systems access to appropriate personnel.

e. Controls are implemented which limits access to files, programs, and data to users or groups of users with the same need-to-know. Need-to-know shall be based on functional responsibilities, operational requirements, supervisory responsibilities, or a combination of these factors.

f. The System Administrator with the help of the SISSO is to ensure that all security updates and patches are evaluated and approved as appropriate.

g. All security software that was provided as part of the original system configuration (e.g., audit trail) is installed and operational.

h. Each system user is assigned a valid and appropriate logon procedure to control the processing options available to the system user.

E. Custodial Requirements

The Program Managers will ensure unauthorized custodial and building maintenance personnel entering areas designated as a Sensitive Computer Area (SCA), are under continual observation by personnel with authorized unescorted access. [NOTE: The SISSO is responsible for identifying all SCAs within his jurisdiction. Typically, an SCA would include those areas where servers, routers, or other networking hardware devices are put into operation.]

1. The SISSO will develop and maintain a list of personnel who will be granted unescorted access into the SCA.

2. The SISSO must maintain a visitors' log for all persons entering the SCA who do not have unescorted access privileges. Only personnel listed on the "Authorized Access List" will escort visitors. Individuals not on the "Authorized Access List" must sign the visitors' log prior to being allowed access into the SCA. While in the SCA, visitors must be under continuous visual observation by a person with authorized unescorted access.

F. Telecommunication Requirements

Users will not physically connect via modem, Internet service providers, or other means, personally owned microcomputers or communication devices to U.S. Government owned systems or communication devices within OSM facilities, without the prior authorization of the system administrator. It is understood that authorization for connection may be granted if said connectivity is necessary for systems or applications development testing.

1. Bureau employees and/or users having system accounts will not physically connect via modem, Internet service providers, or other means to government owned computers, workstations, servers, routers or any other computing or telecommunication devices without the prior written authorization from appropriate LAN administrators or system administrators responsible for the system. The LAN or System administrator may grant a temporary exception if said connectivity is necessary for official systems or applications development requiring testing of telecommunication

capabilities. This authorization will be of a temporary nature, and once tested, the restriction against outside connectivity will be put back in place.

2. Bureau employees and/or users having system accounts may not automatically forward e-mail from Government e-mail systems to personal or remote systems without the express written authorization of the LAN administrator. Message forwarding of this type might be used to inadvertently telecommunicate secure or sensitive government data to an insecure or inappropriate location.

3. Bureau employees and/or users having system accounts may not set up remote access capabilities to control or monitor government computers from remote locations (unless said remote locations are at authorized government offices) without the express written authorization of LAN or system administrators. Failure to follow this procedure could result in compromise by an insecure telecommunications connection. For example, an employee of the Bureau may not run a PC-anywhere type of application from his or her office computer that would accept a connection from the employee's home computer, without the express written authorization of the LAN or system administrator. The LAN or system administrator is authorized to grant a connection of this nature only after performing a review of the need and assessment of security measures in place.

G. Evaluation Requirements

The Information Security Officers Review Team (iSORT) will periodically evaluate capabilities, and, where necessary, implement procedures, to address state of the art encryption techniques to help ensure the integrity of system level passwords when transmitted over the network.

System Owners must periodically review the access privileges of each application user under their jurisdiction to verify system access privileges originally granted are still appropriate.

H. Software and Applications Requirements

1. The Program Manager will ensure that only OSM approved or distributed versions of customized agency or corporate application software (microcomputer software excluded) are used on computer systems and networks owned or operated by OSM.

2. Authorized application developers are the only personnel authorized to modify OSM standard application software.

3. Employees developing application software for OSM systems, will develop and document their application software in accordance with industry standards and practices.

4. The Supervisor will ensure that personally owned software, shareware or freeware are not installed on computer systems owned or operated by OSM without the approval of the Supervisor and IT support.

5. All software must be scanned for viruses and other malicious programming code prior to installation on any computer system or network owned or operated by the OSM. Virus scanning software will be installed on all workstations and microcomputers in the OSM.

Appendix A1. Information Systems Security Quick Reference Guide

Minimum Security Requirements	**Act 1987***	**A-130**	**A-123 A-127**	**CFR**	**FIRMR**	**PA/ FOIA**	**NIST Pubs**
Program Responsibilities Implement and maintain ISSP; assign responsibilities.		X			X	X	
Security Plans Identify sensitive systems; implement security plans.	X				X		800-18
Applications Security Review applications systems every 3 years. Develop and maintain contingency plans.		X X	X		X X		73, 102 87
Installation Security Conduct risk analysis every 5 years. Prepare acquisition specifications. Maintain disaster recovery plans.		X X X	X		X X X		31, 65 87
Personnel Security Designate all positions and screen incumbents.		X		X	X		
Security Awareness and Training Train Federal and contractor personnel.	X	X					500-172
Reporting Report security weaknesses in A-123 Report to President.		X	X				

Appendix A2. Reference Detail Listings

A. Public Policy and Law

Computer Crime Act of 1984.

Computer Security Act of 1987, P.L. 100-235 (1988).

Concealment, Removal, or Mutilation Generally, 18 U.S.C. 1071 (1948).

Disclosure of Confidential Information Generally, 18 U.S.C. 1905 (1948).

Federal Manager's Financial Integrity Act of 1982, P.L. 97-255, 31 U.S.C. 66a (1982).

Interception and Disclosure of Wire or Oral Communications Prohibited, 18 U.S.C. 2511 (1968).

Malicious Mischief, 18 U.S.C. 1361 (1967).

Paperwork Reduction Act of 1980, P.L. 96-511, 44 U.S.C. 3501-3520 (1980), as amended in the Paperwork Reauthorization Act.

Privacy Act of 1974, P.L. 93-579, 5 U.S.C. 552a (1974).

Public Money, Property, or Records, 18 U.S.C. 641 (1948).

B. Office of Management and Budget

OMB Circular A-11, "Preparation and Submission of Budget Estimates," June 17, 1988.

OMB Circular A-109, "Major Systems Acquisitions," April 5, 1976.

OMB Circular A-123, Revised, "Internal Control Systems," August 4, 1986.

OMB Circular A-127, "Financial Management Systems," December 19, 1984.

OMB Circular A-130, "Management of Federal Information Resources," December 12, 1985.

OMB Bulletin No. 90-08, "Guidance for Preparation of Security Plans for Federal Computer Systems that Contain Sensitive Information," July 9, 1990.

OMB *Internal Control Guidelines*, December 1982.

"OMB Revised Supplemental Guidance for Conducting Computer Matching Programs," FR 47, 21656-21658, May 19, 1982.

C. General Accounting Office

Executive Guide, Information Security Management, May 1998

D. General Services Administration

Federal Information Resources Management Regulation (FIRMR), 1990.

Federal Procurement Management Regulations.

GSA Handbook, "Federal ADP and Telecommunications Standards Index."

FIRMR Bulletin C-22, "Security and Privacy Protection of Federal Information Processing (FIP) Resources," September 18, 1992.

FIRMR Bulletin C-28, "Computer Viruses," November 6, 1990.

41 *Code of Federal Regulations* (CFR) Subparts 1-4.11, "Procurement and Contracting Government-wide for Automated Data Processing, Equipment, Software, Maintenance Services, and Supplies."

E. Office of Personnel Management

5 CFR 731 "Suitability."

5 CFR 732, "National Security Positions."

5 CFR 736 “Personnel Investigations”

5 CFR Part 930, "Training Requirements for the Computer Security Act."

36 CFR Part 1234 “Electronic Records Management”

F. National Institute of Standards and Technology

CSC_STD-003-85, “Guidance For Applying The Bureau Of Defense Trusted Computer System Evaluation Criteria In Specific Environments,” June 25, 1985.

DOD 52200.28 STD, “Trusted Computer Systems Evaluation Criteria,” December 1985.

Federal Information Processing Standards Publication (FIPS) 11-3, *American National Dictionary for Information Systems*, February 1991.

FIPS PUB 31, *Guidelines for Automated Data Processing Physical Security and Risk Management*, June 1974.

FIPS PUB 38, *Guidelines for Documentation of Computer Programs and Automated Data Systems*, February 1976.

FIPS PUB 41, *Computer security Guidelines for Implementing the Privacy Act of 1974*, May 1975.

FIPS PUB 46-1, *Data Encryption Standard*, January 1988.

FIPS PUB 48, *Guidelines on Evaluation Techniques for Automated Personnel Identification*, April 1977.

FIPS PUB 64, *Guidelines for Documentation of Computer Programs and Automated Data Systems for the Initiation Phase*, August 1979.

FIPS PUB 65, *Guideline for Automated Data Processing Risk Analysis*, August 1979.

FIPS PUB 73, *Guidelines for Security of Computer Applications*, June 1980.

FIPS PUB 74, *Guidelines for Implementing and Using the NBS Data Encryption Standard*, April 1981.

FIPS PUB 81, *DES Modes of Operation*, December 1980.

FIPS PUB 83, *Guideline on User Authentication Techniques for Computer Network Access Control*, September 1980.

FIPS PUB 87, *Guidelines for ADP Contingency Planning*, March 1981.

FIPS PUB 88, *Guideline on Integrity Assurance and Control in Database Administration*, August 1981.

FIPS PUB 101, *Guideline for Lifecycle Validation, Verification, and Testing of Computer Software*, June 1983.

FIPS PUB 102, *Guideline for Computer Security Certification and Accreditation*, September 1983.

FIPS PUB 112, *Password Usage*, May 1985.

FIPS PUB 113, *Computer Data Authentication*, May 1985.

FIPS PUB 132, *Guideline for Software Verification and Validation Plans*, November 1987.

FIPS PUB 139, *Interoperability and Security Requirements for Use of the Data Encryption Standard in the Physical Layer of Data Communications*, August 1983.

FIPS PUB 140, *General Security Requirements for Equipment Using the Data Encryption Standard*, April 1982.

FIPS PUB 141, *Interoperability and security Requirements for Use of the Data Encryption Standard with CCIT Group 3 Facsimile Equipment*, April 1985.

FIPS PUB 146-1, *Government Open Systems Interconnection Profile (GOSIP)*, April 1991.

FIPS PUB 171, *Key Management Using X9.17*, April 1992.

FIPS PUB 180, *Secure Hash Standard*, May 1993.

FIPS PUB 181-1, *Digital Signature Standards (DSS),* December 1998.

FIPS PUB 191, *Guidelines for the Analysis of Local Area Network Security,* November 1994.

FIPS PUB 196, *Entity Authentication Using Public Key Cryptography,* February 1997.

Special Publication (SPEC PUB) 500-109, *Overview of Computer security Certification and Accreditation*, April 1984.

SPEC PUB 500-120, *Security of Personal Computer Systems: A Management Guide*, January 1985.

SPEC PUB 500-133, *Technology Assessment: Methods for Measuring the Level of Computer Security,* October 1985.

SPEC PUB 500-134, *Guide on Selecting ADP Backup Process Alternatives,* November 1985.

SPEC PUB 500-136, *An Overview of Computer Software Acceptance Testing,* February 1986.

SPEC PUB 500-137, S*ecurity for Dial-Up Lines,* May 1986.

SPEC PUB 500-153, *Guide to Auditing for Controls and security: A System Development Life Cycle Approach*, April 1988.

SPEC PUB 500-157, *Smart Card Technology: New Methods for Computer Access Control*, September 1988.

SPEC PUB 500-161, *Software Configuration Management: An Overview*, March 1989.

SPEC PUB 500-166, *Computer Viruses and Related Threats: A Management Guide*, August 1989.

SPEC PUB 500-169, *Executive Guide to the Protection of Information Resources*, October 1989.

SPEC PUB 500-170, *Management Guide to the Protection of Information Resources*, October 1989.

SPEC PUB 500-171, *Computer User's Guide to the Protection of Information Resources,* October 1989.

SPEC PUB 500-173, *Guide to Data Administration*, October 1989.

SPEC PUB 500-174, *Guide to Selecting Automated Risk Analysis Tools*, October 1989.

SPEC PUB 500-180, *Guide to Software Acceptance*, April 1990.

SPEC PUB 800-3, *Establishing a Computer Security Incident Response Capability* (CSIRC), November 1991.

SPEC PUB 800-4, *Computer Security Considerations in Federal Procurements: A Guide for Procurement Initiators, Contracting Officers, and Computer Security Officials,* March 1992.

SPEC PUB 800-5, *A Guide to the Selection of Anti-Virus Tools and Techniques*, December 1992.

SPEC PUB 800-6, *Automated Tools for Testing Computer System Vulnerability*, December 1992.

SPEC PUB 800-7, *Security In Open Systems,* July 1994.

SPEC PUB 800-10, *Keeping Your Site Comfortably Secure: An Introduction to Internet Firewalls,* December 1994.

SPEC PUB, 800-12, *An Introduction to Computer Security: The NIST Handbook,* October 1995.

SPEC PUB, 800-13, *Telecommunications Security Guidelines for Telecommunications Management Networks,* October 1995.

SPEC PUB 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems,* June 1996.

SPEC PUB 800-16, *Information Technology Security Training Requirements: A Role and Performance Based Model,* March 1998.

SPEC PUB 800-18, *Guide for Developing Security Plans for Information Technology Systems,* December 1998.

NISTIR 4636, *U.S. Dept. of Health and Human Services (HHS) Information Systems Security Handbook*, July 1991.

NISTIR 4659, *Glossary of Computer Security Terminology*, September 1991.

NISTIR 4749, *Sample Statements of Work for Federal Computer Security Services: For Use In-House or Contracting Out*, December 1991.

NISTIR 4846, *Computer Security Training & Awareness Course Compendium*, May 1992.

NISTIR 4939, *Threat Assessment of Malicious Code and External Attacks*, October 1992.

NISTIR 4976, *Assessing Federal and Commercial Information Security Needs*, November 1992.

NISTIR 5153, *Minimum security Requirements for Multi-User Operating Systems*, March 1993.

NIST Publication List 58, *FIPS PUBS Index*.

NIST Publication List 88, *Computer Systems Publications*.

NIST Publications List 91, *Computer Security Publications.*

G. National Telecommunication and Information Systems Security

NTISS Directive 900 "Governing Procedures Of The National Telecommunication And Information Systems Security (NTISS) Committee," March 1, 1985, and subsequent directives and guidelines to be issued by NTISS Committee.

H. Office of Surface Mining Reclamation and Enforcement

Information Systems Life Cycle Guidance, INF-11

Computer Users Guidance Manual, June 1999

I. DOI

375 DM 19, *DOI Security Manual.*

441 DM 1-6**,** *Personnel Suitability and Security Investigation Requirements*

444 DM 1, *Physical Protection and Building Security.*

442 DM 1-15**,** *National Security Information*

J. Other

Department Of Commerce, RP-1, *Standard Practice For The Fire Protection Of Essential Electronic Equipment Operations,* 1978

Department of Commerce, RP-1, *Standard Practice for the Fire Protection of Essential Electronic Equipment Operations*, 1978.

Lawrence Livermore National Laboratory UCRL-ID-104689, *Responding to Computer Security Incidents: Guidelines for Incident Handling*, July 1990.

Microsoft Press Computer Dictionary: The Comprehensive *Standard for Business, School, Library, and Home*. Redmond, WA: Microsoft Press, 1991.

NFPA, Publication 75-1992, *Protection of Electronic Computer/Data Processing Equipment*, 1992.

NISTIR 4659, *Glossary of Computer Security Terminology,* September 1991.

President's Council on Management Improvement and the President's Council on Integrity and Efficiency, *Model Framework for Management Control Over Automated Information Systems.* Washington, DC: GPO, 1988.

Appendix B. Definitions

ACCESS TO INFORMATION Access to information refers to the function of providing to members of the public, upon their request, the Government information to which they are entitled under law. (OMB Circular A-130)

APPLICATION SYSTEM An application system is a computer system written by or for a user that applies to the user's work; for example, a payroll system, inventory control system, or a statistical analysis system. (FIPS PUB 11-3)

APPLICATION SYSTEM MANAGER An Application System Manager is the official who is responsible for the operation and use of an application system. (OSM Definition)

COMPUTER SECURITY INCIDENT RESPONSE CAPABILITY (CSIRC) A CSIRC is that part of the computer security effort that provides the capability to respond to computer security threats rapidly and effectively. [A CSIRC provides a way for users to report incidents, and it provides personnel and tools for investigating and resolving incidents, and mechanisms for disseminating incident-related information to management and users. Analysis of incidents also reveals vulnerabilities, which can be eliminated to prevent future incidents.] (NIST SPEC PUB 800-3)

COMPUTER SYSTEM Any equipment or interconnected system or subsystems of equipment used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information; including computers; ancillary equipment; software, firmware, and similar procedures; services, including support services; and related resources as defined by regulations issued by the Administrator for General Services pursuant to section 111 of the Federal Property and Administrative Services Act of 1949. (Computer Security Act of 1987)

COMPUTER SYSTEMS SECURITY PLAN (CSSP) The CSSP provides a basic overview of the security and privacy requirements of the subject system and the agency's plan for meeting those requirements. (OMB Bulletin 90-08)

CONTINGENCY PLAN A contingency plan is a plan for emergency response, backup procedures, and post-disaster recovery. Synonymous with disaster plan and emergency plan. (FIPS PUB 11-3)

DATA COMMUNICATIONS Data communication is the transfer of data between functional units by means of data transmission according to a protocol. (FIPS PUB 11-3)

DATABASE A database is a collection of interrelated data, often with controlled redundancy, organized according to a schema to serve one or more applications; the data are stored so that different programs without concern for the data structure or organization can use them. A common approach is used to add new data and to modify and retrieve existing data. (FIPS PUB 11-3)

DATABASE MANAGER A Database Manager is the official who is responsible for the operation and use of a database. (OSM Definition)

DISSEMINATION OF INFORMATION Dissemination of information refers to the function of distributing Government information to the public, whether through printed documents, or electronic or other media. Dissemination of information does not include intra-agency use of information, inter-agency sharing of information, or responding to public requests for access to information. (OMB Circular A-130)

FEDERAL COMPUTER SYSTEM A Federal computer system is a computer system operated by a Federal agency or by a contractor of a Federal agency or other organization that processes information (using a computer system) on behalf of the Federal Government to accomplish a Federal function. A Federal computer system includes automatic data processing equipment as that term is defined in section 111(a)(2) of the Federal Property and Administrative Services Act of 1949. (Computer Security Act of 1987)

GOVERNMENT INFORMATION Government information is any information that is created, collected, processed, transmitted, disseminated, used, stored, or disposed of by the Federal Government. (OMB Circular A-130)

INFORMATION Information is any communication or reception of knowledge, such as facts, data, or opinions, including numerical, graphic, or narrative forms, whether oral or maintained in any other medium, including computerized databases, paper, microform, or magnetic tape. (OMB Circular A-130)

INFORMATION SYSTEM (IS) An IS is the organized collection, processing, transmission, and dissemination of automated information in accordance with defined procedures. (OMB Circular A-130)

INFORMATION RESOURCES MANAGEMENT (IRM) IRM is the planning, budgeting, organizing, directing, training, and control associated with Government information. The term encompasses both the information itself and related resources, such as personnel, equipment, funds, and technology. (OMB Circular A-130)

INFORMATION SYSTEM SECURITY [COMPUTER SECURITY] Information system security refers to the concepts, techniques, technical measures, and administrative measures used to protect the hardware, software, and data of an information processing system from deliberate or inadvertent unauthorized acquisition, damage, destruction, disclosure, manipulation, modification, use, or loss. (FIPS PUB 11-3)

INFORMATION SYSTEMS SECURITY (INFOSEC) An INFOSEC is the protection afforded to information systems to preserve the availability, integrity, and confidentiality of the systems and information contained in the systems. [Protection results from the application of a combination of security measures, including crypto-security, transmission security, emission security, computer security, information security, personnel security, resource security, and physical security.] (NISTIR 4659)

INFORMATION TECHNOLOGY FACILITY An information technology facility is an organizationally defined set of personnel, hardware, software, and physical facilities, a primary function of which is the operation of information technology. [Information technology facilities range from large centralized computer centers to individual stand-alone microcomputers.] (OMB Circular A-130)

MALICIOUS SOFTWARE Malicious software is the collective name for a class of programs intended to disrupt or harm systems and networks. The most widely known example of malicious software is the computer virus; other examples are Trojan horses and worms. (OSM Definition, adapted from NIST SPEC PUB 500-166)

PERSONNEL SECURITY Personnel security refers to the procedures established to ensure that each individual has a background which indicates a level of assurance of trustworthiness which is commensurate with the value of information technology resources which the individual will be able to access. (NISTIR 4659)

PHYSICAL SECURITY Physical security refers to the application of physical barriers and control procedures as preventive measures and countermeasures against threats to resources and sensitive information. (NISTIR 4659)

RISK ASSESSMENT A risk assessment is the identification and study of the vulnerability of a system and the possible threats to its security. (FIPS PUB 11-3)

RISK MANAGEMENT Risk management is the process of identifying, controlling, and eliminating or minimizing uncertain events that may affect system resources. It includes risk analysis, cost benefit analysis, selection, implementation and test, security evaluation of safeguards, and overall security review. (NISTIR 4659)

SENSITIVE APPLICATION A sensitive application is an application of information technology that requires protection because it processes sensitive data, or because of the risk and magnitude of loss or harm that could result from improper operation, deliberate manipulation, [or delivery interruption] of the application. (OMB Circular A-130)

SENSITIVE COMPUTER AREA (SCA) Would include those areas where servers, routers or other networking devices are put into operation.

SENSITIVE DATA Sensitive data are data that require protection due to the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the data. The term includes data whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary data, records about individuals requiring protection under the Privacy Act, and data not releasable under the Freedom of Information Act. (OMB Circular A-130)

SENSITIVE INFORMATION Sensitive information is any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect OSM.

SIGNIFICANT CHANGE A significant change is a physical, administrative, or technical modification that alters the degree of protection required. Examples include adding a local area network, changing from batch to on-line processing, adding dial-up capability, and increasing the equipment capacity of the installation. (OSM Definition)

USER A user is any organizational or programmatic entity that [utilizes or] receives service from an [automated information system] facility. A user may be either internal or external to the agency organization responsible for the facility, but normally does not report to either the manager or director of the facility or to the same immediate supervisor. (OMB Circular A-130)

Appendix C. Acronyms

ANACI	**Access National Agency Check and Inquires Investigation**
BI	**Background Investigation**
CERTeam	**Computer Emergency Response Team**
COTR	**Contracting Office Technical Representative**
CSIRC	**Computer Security Incident Response Capability**
CSSP	**Computer Systems Security Plan**
DCIO	**Deputy Chief Information Office for Information Resources Management**
FedCIRC	**Federal Computer Incident Response Center**
FIPS PUB	**Federal Information Processing Standards Publication**
FIRMR	**Federal Information Resources Management Regulation**
FPPS	**Federal Personnel Processing System**
ICR	**Internal Controls Review**
IS	**Information Systems**
iSORT	**Information Security Officer Review Team**
ISSO	**Information Systems Security Office**
ISSP	**Information Systems Security Program**
IT	**Information Technology**
NACI	**National Agency Check and Inquiries Investigation**
NACIC	**National Agency Check and Inquiries plus Credit Check Investigation**
NACLC	**National Agency Check with Law and Credit Investigation**
NARA	**National Archives and Records Administration**
NFPA	**National Fire Protection Association**
NIST	**National Institute of Standards and Technology**
NSS	**Network System Support, at Headquarters**
PM	**Program Managers**
SISSO	**Site Information Systems Security Officer**
SSBI	**Single Scope Background Investigation**
SPEC PUB	**(NIST) Special Publication**

recognize and assess the threats and vulnerabilities to automated information resources so that the responsible managers can set security requirements which implement Agency security policies.

d. **Performance level training.** Provides employees with skill to design, execute, or evaluate Agency computer security policies and practices so that employees will be able to apply security concepts while performing tasks that relate to their duties and positions.

IS Training and Orientation Requirements below, adapted from the NIST Training Matrix, provides an overview of the content and appropriate training level for each of the target populations. Subject areas, target populations, and training levels are described in detail following the chart:

	TRAINING AREA				
AUDIENCE CATEGORY	Computer Security Basics	Security Planning & Management	Computer Security Policy & Procedures	Contingency Planning	Systems Life Cycle Management
Executives	Awareness	Policy	Awareness	Awareness	Awareness
Program Managers	Awareness	Implementation	Implementation	Performance	Performance
ISSO, SISSO	Awareness	Performance	Performance	Performance	Performance
LAN, Application System, System, and Database Managers	Awareness	Performance	Performance	Performance	Performance
Users	Awareness	Awareness	Performance	Performance	Awareness

4. Training is an ongoing process and, at a minimum, should be provided whenever there is a significant change in the Agency's information security environment or procedures, or when an employee enters a new position that deals with sensitive information.

All Site ISSO's should receive advanced formal computer training. User training should include security awareness as part of their existing computer training, management courses, and employee orientation. Modes of delivery outside the classroom are acceptable; e.g., computer assisted training, videotapes, workbooks, job aids, and desk guides.

5. Computer security refresher training should be provided annually or as frequently as determined necessary by the Agency, based on the sensitivity of the information that the employee uses or processes.

Chapter VIII. IT Facilities

A. Overview

In accordance with the OSM Information Systems Security Program, all OSM organizations that operate Information Technology (IT) facilities must implement physical security and operating safeguards to protect these assets from unauthorized or fraudulent use, manipulation, or destruction. This chapter presents policies and guidelines for protecting computer facilities and operating systems at the organizational level. The goal is to protect and preserve information, human assets, physical assets, and operating systems by reducing their exposure to vulnerabilities that can disrupt or curtail information systems operations.

The Bureau's information technology facilities are categorized as follows:

1. Government-owned and Government-operated,
2. Government-owned and contractor-operated, and
3. Contractor-owned and contractor-operated.

The policies and guidelines presented in this chapter apply to information technology facilities that house information technology equipment. These policies and guidelines also apply to Local Area Networks (LANs) and to the Wide Area Network (WAN), since the various components of LANs are housed in information technology facilities.

Although stand-alone microcomputers are technically considered to be information technology facilities, they are excluded from the policies and guidelines presented in this chapter, except where specifically referenced, because many of the safeguards discussed in this chapter are not applicable.

B. Physical Security

1. Introduction

In accordance with the OSM Information Systems Security Program, all OSM organizations must implement physical security safeguards to protect the Bureau's information technology resources. These safeguards must be applied in all administrative, physical, and technical areas and can include the use of locks, guards, administrative controls, and measures to protect against damage from intentional acts, accidents, fires, and environmental hazards such as floods, hurricanes, and earthquakes. The minimum safeguards for all information technology facilities are outlined in Chapter III, C, "Matrix of Minimum Security Safeguards." Facilities Management must also ensure that their facilities fully comply with the physical security requirements as defined in NIST Handbook 800-18 and in DOI 444 DM 1, "Physical Protection and Building Security."

The Minimum Security Safeguards reflect the minimum security requirements that must be implemented until a formal risk assessment of an information technology facility has been conducted. Based on the results of the risk assessment, additional safeguards may be added. If the risk assessment shows noncompliance with security requirements, the reasons why the security requirements cannot be met must be documented, and the documentation must be available for inspection. If an organization cannot implement a Federal security requirement or standard, a waiver request may be submitted to the Deputy Chief Information Officer (DCIO). The DCIO will determine whether the waiver request should be forwarded to the appropriate government official for approval.

Before selecting and implementing safeguards to protect the physical security of information technology facilities, the IT Facility Manager should identify the various components of the information technology facility that require protection. These components may include:

a. Computer room

b. Data control and conversation area

c. Programmer's area

d. Terminal/remote entry

e. Communications equipment area

f. Data file storage area

g. Forms storage area

h. Supplies storage area

i. Maintenance/workshop area

j. Support equipment area

k. Telephone closet

l. Power supply area (including transformer vaults and power panels)

m. General office area (where sensitive data is handled)

The selected safeguards should include, but not be limited to, access control, protection of sensitive materials, IS facility construction, and fire safety.

2. Access Control

The IT Facility Manager must establish physical and administrative controls to prevent unauthorized entry into operations, data storage, library, and other support areas. The following actions should be taken in establishing these controls:

a. Physical Controls

Equip all doors in all areas containing information technology equipment with mechanical or electronic locking mechanisms. Emergency and "Exit Only" doors should be equipped with hardware which permits immediate egress in the event of an emergency.

b. Administrative Controls

Develop and implement administrative procedures for limiting IT facility access to authorized personnel only. To achieve this objective, management should:

1. Prepare and maintain access authorization lists.

2. Discourage the presence of visitors. (When a visit is necessary, require an escort at all times).

3. Maintain logs to record the entry and departure of all individuals, other than normally authorized personnel.

4. Coordinate with the building manager to limit the presence of cleaning and maintenance personnel to the period when regular employees are on duty.

5. Establish procedures to record and report occurrences of non-routine user/operator activity, such as:

   a. Terminals left unsecured after-hours.

   b. Doors to information technology facilities, remote job entry facilities, terminal rooms, library, or media storage areas left unlocked after-hours.

6. Where appropriate post "For Authorized Personnel Only" signs where sensitive data are used or stored.

3. Protection of Sensitive Materials

All OSM organizations should establish procedures to control the handling, distribution, storage, disposition, and destruction of materials that contain sensitive data. The Facility Manager should establish physical and administrative controls to prevent unauthorized entry into operations, data storage, library, and other support areas. The following actions should be taken in establishing these controls:

a. Physical Controls

Ensure that all sensitive materials, such as data printouts and other hard copy materials, software documentation, operating manuals, and handbooks, are labeled as sensitive and stored in a secure location when not in use, preferably in a lockable filing cabinet or desk.

b. Administrative Controls

1. Establish procedures to prevent erroneous or unauthorized transfer of sensitive materials.

2. Ensure that storage media containing sensitive data are labeled.

3. Ensure that the Records Liaison Officer maintains a file and disposition plan for all data in the information technology facility, in consultation with the organization's records management officer. The National Archives and Records Administration (NARA) provides general guidelines for the disposition of electronic records. (See 36 CFR 1234, Electronic Records Management)

4. Dispose of all retired, discarded, or unneeded sensitive data in a manner that will prevent unauthorized persons from making use of it.

a. Ensure that all sensitive data are erased from storage media prior to repair or before release as work tapes, disks, or memory areas (degaussing).

b. Ensure the secure destruction of all sensitive hard copy documents when they are no longer needed.

5. Protect sensitive data during an external evaluation.

4. Facility Construction

The Facility Manager and SISSO must review the construction plans for all new information technology facilities, and for modifications to existing information technology facilities, to determine the most cost-effective method for securing the facilities. The potential vulnerability of the facility to penetration by outside forces, the sensitivity of the data to be processed, and the value of the equipment to be protected should be considered in making this determination.

Minimum protection must be provided for all new information technology facilities and modifications to existing IS facilities using the following guidelines:

a. Walls should be constructed of materials that offer resistance to forced entry and have a fire rating of at least one hour. (Refer to GSA FPMR Subpart 101.36.7 and the Bureau of Commerce RP-1, Standard Practice for the Fire Protection of Essential Electronic Equipment Operations.)

b. All facility doors should be constructed of materials that are comparable to the facility walls in strength and fire rating.

c. The most desirable location in which to house information technology equipment is an interior room, above the first floor, having four solidly constructed walls that extend from the true floor to the true ceiling. Location and construction are particularly important if the information technology equipment will not be attended on a 24-hour basis. Attended information technology equipment requires only a minimum level of protection, since resident personnel easily detect unauthorized access.

d. Basement, first and second floor windows, and windows accessible from adjacent structures should be secured when the facility is unattended. The replacement of glass windows with plastic windows should be considered. If the information technology facility is a potential target for vandalism, windows should be barred, screened, or opaque.

5. Fire Safety

SISSO must ensure that appropriate safeguards are implemented to prevent, detect, and/or suppress fires and protect IT equipment in the event of a fire. The following safeguards are required to ensure fire safety, and many of them will also reduce vulnerability to other environmental hazards. For further guidance on fire safety, refer to Department of Commerce RP-1, *Standard Practice for the Fire Protection of Essential Electronic Equipment Operations*, the National Fire Protection Association (NFPA) Publication 75-1992, *Protection of Electronic Computer/Data Processing Equipment*, and local ordinances and building codes.

Chapter IX. Integrating Computer Security into the System Life Cycle

Overview

The National Institute of Standards and Technology (NIST) defines the system life cycle as "the period of time beginning when the software product is conceived and ending when the resultant software products are no longer available for use. The [system life cycle] is typically broken into phases, such as requirements, design, programming and testing, installation, and operations and maintenance. Each phase consists of a well-defined set of activities whose products lead to the evolution of the activities and products of each successive phase."

Information security should be integrated into the application system life cycle from its inception for several reasons:

1. **It is less expensive.** To retrofit security is generally more expensive than to integrate it into an application.

2. **It is more effective.** Meaningful security is easier to achieve when security issues are considered as part of a routine development process, and security safeguards are integrated into the system during its design.

3. **It is less obtrusive.** When security safeguards are integral to a system, they are usually easier to use and less visible to the user.

For more in-depth discussion of life cycle issue, see NIST 800-18, Chapter 44.

Chapter X. Desktop, Software and Systems

A. Overview

This chapter presents the Information Systems Security Program (ISSP) policy for protecting microcomputers and microcomputer application systems and data from damage, destruction, or misuse. The term "microcomputers" includes workstations, personal computers (PCs), other desktop computers, laptops, notebooks, palmtops, and other portables, such as personal digital assistants and personal organizers.

The requirements of this chapter apply to all organizations that use microcomputers. Additional requirements apply for microcomputers that:

1. Use software developed by the user

2. Communicate with other microcomputers.

This policy also applies to microcomputers owned by OSM but authorized for work outside the office by OSM employees, and microcomputers owned by OSM employees but used for official work-related purposes.

Protecting and safeguarding microcomputer software and data can be a difficult problem, since microcomputers are generally easy to access. Therefore, subject to Federal regulations and penalties, all Application System Managers, supervisors, and microcomputer users are responsible for taking actions to safeguard and prevent the improper use of, damage to, or destruction of microcomputer data, application systems, and hardware. The extent of these actions should be commensurate with the sensitivity of the data, operational criticality of the application systems, the value of the hardware, and the distribution of functions and authority.

B. Controlling Access to Systems

1. The System Manager controls and limits computer system access to individuals requiring system access in the performance of their official duties. The IT Specialist/System Manager must limit the access of system users to the minimum level necessary to perform their official duties.

2. Supervisors must complete a written access request for each staff member requiring system access.

3. The System Manager must review each request for accuracy and technical anomalies and retain the request in central files.

4. Prior to gaining access to any of OSM's computer systems or networks,

each user must agree, in writing, to abide by all OSM computer security policies, procedures and guidelines. This documentation is maintained at the local level.

5. Program managers will determine who within their organization requires access to computer systems. This determination will be indicated by written request.

6. System Managers, sometimes referred to as System Owners, or the designated individual, will terminate user system access upon notification by the user's.

C. Specific Requirements for Externally-Developed Software

1. Only software authorized for business purposes should be used on Federal computers.

2. The use of software purchased by the Government is governed by the terms and agreements established by the software vendors and the OSM procurement process. Opening shrink-wrap coverings can constitute acceptance of the licensing terms stated by the vendor. Employees and contractors are strictly forbidden to use or copy software in a manner contrary to licensing agreements and OSM procurement policies. Infringement of software copyrights may constitute theft.

3. PC software products may not be copied more than the limit provided by contract (e.g., including an archived copy for backup purposes). Employees or contractors who make additional copies to avoid the cost of acquiring software must be held accountable for their actions.

4. Superseded PC software may be taken home by employees only if to do so is permitted by the site-license agreement and approved by management. Management approval should depend on the employee's need to perform official government work at home.

5. Software packages protected by quantity licenses must be tracked to control the copying and distribution of the proprietary software.

6. Application System Managers should introduce and enforce management guidelines to prevent the introduction of malicious software into the work place. (See Chapter XII, "Malicious Software and Intrusions.") In general, only shrink-wrapped software or certified shareware should be used. Application System Managers must forbid the use of software downloaded from external sources (e.g. Internet and bulletin boards), unless the downloaded software has first been checked and approved.

D. Information System Security Checklist for Microcomputers

Explanation: The following questions highlight the information system security requirements for application systems that run on microcomputers. For each "NO" response, provide a written explanation on additional paper for the Application System Manager's files.

REQUIREMENTS	YES	NO
1. Do you maintain an accurate inventory of hardware and software?		
2. Are reports and diskettes properly stored in a secure location when not in use?		
3. Do you maintain and update a list of authorized users?		
4. Have the authorized users been trained in both the operation and use of the microcomputer, as well as in Automated system security requirements?		
5. Are application system access passwords available only to authorized users?		
6. Are the passwords changed when authorized employees leave OSM?		
7. When changes are introduced (e.g., new applications, personnel turnover, telecommunications), are risks re-examined?		
8. Are data files backed up periodically? If so, note how often.		
9. Are both user and software documentation kept current and safeguarded?		
10. Where authorized, is software backed up and the original stored in a safe place?		
11. Do you re-examine security on a quarterly basis?		
12. Are security devices installed and procedures in place, which lessen the risk of theft or unauthorized access to the microcomputer?		
13. Are surge suppressors installed?		
14. Are needed contingency plans in place for microcomputers?		
15. Are sensitive data stored or processed on the microcomputer? (If the answer is "no", proceed to question 17.)		
16. Have employees in computer-related personnel positions, which involve the use of microcomputers, undergone appropriate background investigations?		
17. Has password protection capability been implemented to protect the application system? To protect data?		
18. Are sensitive data protected from unauthorized viewing or use during transmission and storage?		
19. Are reports and diskettes labeled and controlled?		
20. Are unneeded sensitive reports shredded and unnecessary files written over?		

NOTE: Individuals who conduct information system security reviews may request specific documentation in support of your responses. In addition, the results of completing this checklist should be used to determine if sensitive information is processed and/or a Computer Systems Security Plan needs to be developed (or updated).

______________________________ ________________

(Signature of Application System Manager) (Date)

______________________________ ________________

(Signature of Organization Information
Systems Security Officer) (Date)

Chapter XI. Data Communications, Networks, E-Mail, Servers and WAN

A. Overview

This chapter presents Bureau policy for protecting sensitive data that are transmitted by electronic means. The policy applies to all OSM organizations which use data communications equipment to transmit automated data and to contractors who provide any type of automated data communication service, software, or equipment. It applies to all telecommunications technology, Local Area Networks (LANs) and the Wide Area Network (WAN).

Data communications encompass the methods, mechanisms, and media involved in information transfer. Two methods of electronic computer communications exist: temporary connection of two computers via modems, and permanent or semi-permanent linking of multiple workstations or computers on a network. The distinction between the two methods, however, is blurred because microcomputers equipped with modems are often used to connect to both privately owned and public access network computers.

Modem-to-modem communications typically involve dial-in access via public telephone lines to a mainframe or a network. Networks, on the other hand, rely on dedicated phone lines and switching systems or, in the case of LANs, machine-to-machine cabling. Networks tend to use sophisticated transport mechanisms and error-catching procedures to route and store messages sent to and from authorized users.

B. Policy

Every OSM organization must identify its sensitive electronic data and provide effective and appropriate protection for data to be transmitted electronically. The Site Information Systems Security Officer and telecommunications officials in the organization must:

1. Ensure that appropriate data communication controls and safeguards are operating in support of each application system and/or automated system that uses data communications.

2. Determine the appropriateness and adequacy of these controls and safeguards to the needs and data sensitivity of the application system or information system.

3. Verify that the controls and safeguards actually function as specified.

4. Identify and implement changes to these controls and safeguards, as required by changing needs and technology.

5. Insure users are instructed to scan for viruses whenever introducing

programs or data external to OSM's networks, for example, floppy discs brought in from home, downloading public domain software.

OSM and contractor personnel must comply with security measures in OMB Circular A-130 and the DOI Security Manual 375 DM 19. Those documents include responsibilities that must be followed by all OSM personnel. In addition, OSM and contractor personnel working for OSM while using the Internet:

a. Must not be harassing, libelous or disruptive to others while connected to the Internet. Fraudulent, harassing or obscene messages and/or materials are not to be sent, printed, requested or stored.

b. Must not transmit personal data or unauthorized government-owned data across the Internet.

c. Must not knowingly download to government computers any obscene written material or pornography.

c. Must obey all copyright laws.

e. Must not send hateful, threatening, or harassing messages.

f. Must not deliberately attempt to degrade the performance of an information system (including computers, microcomputers, networks and telephone systems), or to deprive authorized personnel of resources or access to OSM Information Systems.

g. Must use OSM sponsored Internet connections for official OSM business only, except for the DOI policy allowing personal use of the Internet during non-work hours.

Local Area Networks

a. The LAN at each OSM office will be under the control of the local LAN administrator, who will coordinate with other OSM LAN administrators in supporting OSM staff's network needs.

b. LAN Administrators will coordinate and cooperate with the OSM IRM Coordinator at Headquarters to ensure that OSM networks inter-operate properly, and that OSM users will use those networks to exchange data in compatible formats.

c. All communications will be through the office networks, except for those applications that a user needs access to that are only available via dial-up. The System Owner must grant approval for access to such applications.

d. All LAN user accounts will require passwords, and will require a password change every 90 days. Passwords must not be reused, and shall consist of a combination of letters and numbers and will be a minimum of six characters long. Users are responsible for safeguarding their passwords. They will not be printed, stored online, or given to others. **Users are responsible for all transactions made using their passwords.** No User may access the LAN with another User's password or account.

g. Special support software/hardware may be installed on OSM computing systems and networks in order to support usage accounting, security, network management, hardware and software inventory and updating functions, and to provide better support to personnel. Authorized OSM personnel, and it's contractors, may access other data fields when necessary for maintenance and security of information systems. Advanced notification of access will be given, except for cases precluded by security and maintenance emergencies. When performing maintenance, every effort will be made to ensure the privacy of user files. However, if violations of policies are discovered, they will be reported to Management.

h. To ensure security, users will not connect a modem or any other network circuit to any OSM LAN for the purpose of gaining access without the consent of the LAN Administrator.

i. Each User must ensure the security of the OSM LANs and attached computer resources. This duty includes taking reasonable precautions to prevent intruders from accessing the agency's LANs without authorization.

h. Each User must take reasonable precautions to ensure he or she does not introduce viruses into an OSM LAN. **To that end, all material received on floppy disk or other magnetic or optical medium and all material downloaded from the Internet, or from computers or networks that do not belong to OSM, *MUST* be scanned for viruses and other destructive programs before being placed onto the LAN.** Users should understand that their home computers and laptops might contain viruses. All disks transferred from these computers to OSM's network MUST be scanned for viruses.

i. Where available, password encryption utilities should be used to prevent malicious or inadvertent disclosure of passwords and to prevent powerful system passwords and accounts from being compromised when traveling across a network, such as the Wide-Area Network and the Internet.

Electronic Mail

a. OSM's electronic mail system will be under the control of the Network Systems Support (NSS) staff in HQ for maintenance purposes.

b. OSM users are encouraged to establish separate passwords for their email accounts, and will be required to do so in order to access their accounts across the Internet via web browser interface.

c. Each local E-mail installation will have the security level set to high.

d. All attachments to email messages, whether sent or received, will be scanned for viruses, by the user, using the virus scanning software installed in the local office.

e. Users will not allow others to use their accounts, except for proxy access granted to enable sharing of information. Users will not leave their email accounts "up" on their PC when away from their desks.

OSM Wide Area Network (OSMNET)

a. OSMNET is under the control of Network Systems Support (NSS).

b. Host-based security will be the primary method of protecting OSM systems. This methodology will be enhanced by packet filtering and/or 'firewalling' as necessary.

c. No connections of any kind will be made to OSMNET without approval of NSS.

d. The protocol of OSMNET will be the Internet Protocol (IP), with some IPX protocol being routed on tail circuits, as approved by NSS. IPX shall not be routed across DOINET or the Internet.

e. The OSMNET is an open network, with security implemented at the individual node level through packet filtering and/or 'firewalling.'

f. Firewalls will be a function of NSS, and not be undertaken by the local nodes without NSS approval.

g. Any security change at the local node will be supported by a Risk Assessment, and a detailed requirements document.

h. Any dial-in connections to OSMNET must be coordinated with the NSS, and be supported by a brief requirements document.

i. Internet connectivity from OSMNET will be controlled by NSS. Individual Internet connections from local nodes will not be allowed.

j. All change requests for OSMNET will have Management approval before being presented to NSS for consideration, security being a foremost consideration.

Internet

The responsibility for protecting OSM resources on the Internet is the responsibility of the NSS and the program offices that have Internet servers available to the public. This policy also applies to contractors.

A fire wall compromise is potentially disastrous to internal security. For this reason, OSM will, as far as practical, adhere to the following stipulations when configuring and using firewalls:

a. OSM will strictly limit incoming access to OSM data and systems by Internet users.

b. Where servers are accessible to the public, and a firewall is used, the Demilitarized Zone (DMZ) concept will be part of the firewall architecture. This concept is not required where local conditions do not warrant its use. Limit firewall accounts to only those absolutely necessary, such as the administrator.

Note: A DMZ is an area between the trusted, or inside, network and the untrusted world of the Internet. The term refers to a physical and technical placement of firewall devices, routers and computers. The DMZ contains routers, firewall and Web servers and perhaps other computers that the outside world is allowed to see. The firewall is what controls the traffic and allows trusted users into the trusted network. Probes by hackers thus occur in this area and not inside the firewall.

c. Remove compilers, editors and other program development tools from the firewall system(s) that could enable a hacker to install Trojan Horse software or backdoors.

d. Do not run any vulnerable protocols on the firewall.

e. Disable the finger command. The finger command can be used to leak valuable user information.

f. Do not permit loopholes in firewall systems to allow friendly systems or users special entrance access. The firewall should not view any attempt to gain access to the computers behind the firewall as friendly. Modems provide a back door to a secure Internet; therefore, the use of modems for anything other than dialing out is expressly prohibited for any network-connected workstations unless authorized by NSS.

g. Disable any feature of the firewall that is not needed, including other network access, user shells, applications and so forth.

h. Firewalls will employ auditing, reporting and notification techniques to track security incidents, keep logs and warn the appropriate security personnel when violations occur.

i. Proxy services and caching improve security levels and can increase efficiency on the network. Therefore, proxy services shall be used where practical and advisable.

The Computer Security Act of 1987 assigned the National Institute of Standards and Technology (NIST) the responsibility for developing computer security standards and guidelines for unclassified Federal systems, including data communications systems and networks.

C. Sample LAN/WAN Security Plan Checklist

Explanation: This checklist is designed to help IRM management, information technology security officers, and LAN officials review security plans for LANs and WAN. It is keyed to the major elements of the Computer Systems Security Plan (CSSP) format as presented in OMB Bulletin 90-08, "Guidance for Preparation of Security Plans for Federal Computer Systems that Contain Sensitive Information."

Yes/No Questions		Yes	No	N/A
1.	Have Computer Systems Security Plans (CSSPs) been implemented for LANs and WANs designated sensitive?			
2.	Does each CSSP contain the following information?			
	a. Name, category, operational status, description and environment adequately identify systems.			
	b. Each CSSP identifies additional applications and systems covered.			
	c. Information sensitivity is identified by type (confidentiality, integrity, and availability) and relative importance (low, moderate, and high).			
	d. The magnitude of potential harm or loss is identified.			
3.	Does each CSSP indicate whether control measures are in place, planned, or not applicable for:			
	a. Assignment of security responsibility			
	b. Risk assessment (within last five years)			
	c. Personnel screening			
	d. Acquisition specifications			
	e. Security and awareness training			
	f. Operational controls:			
	(1) Physical and environmental protection			
	(2) Production and input/output controls			
	(3) Emergency, backup, and contingency planning			
	(4) Audit and variance detection			
	(5) Hardware and system software maintenance controls			

	(6) Documentation			
	g. Technical controls:			
	(1) User identification and authentication			
	(2) Authorization/access controls			
	(3) Integrity controls			
	(4) Audit trail mechanisms			
	(5) Confidentiality controls			

Chapter XII: Malicious Software and Intrusions

A. Overview

Computer systems and communication networks are subject to a variety of threats, many of which have emerged during the past decade with the enormous growth in the use of microcomputers and Local Area Networks (LANs). These threats fall into two categories: malicious software and intrusions.

Malicious software is the collective name for a class of programs intended to disrupt or harm systems and networks. The most widely known example of malicious software is the computer virus.

Intrusions are penetrations of computer systems and networks by hackers. Hackers may be legitimate users who overstep the bounds of authorized access or outsiders who break into systems for which they have no authorization.

B. Malicious Software

A **Trojan horse** is "a destructive program disguised as a game, a utility, or an application. When run, a Trojan horse does something devious to the computer system while appearing to do something useful."

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

A **worm** is "a program that propagates itself across computers, usually by spawning copies of itself in each computer's memory. A worm might duplicate itself in one computer so often that it causes the computer to crash. Sometimes written in separate 'segments', a worm is introduced surreptitiously into a host system either for 'fun' or with intent to damage or destroy information."

C. Intrusions

A hacker is a person "who secretively invades others' computers, inspecting or tampering with the programs or data stored on them." Hackers use a variety of techniques to gain unauthorized access, including:

1. **Password cracking**, in which the hacker tries easily guessed passwords, or uses a dictionary as a source of guesses for an automated attack.

2. **Exploiting known security weaknesses**, in which the hacker takes advantage of vulnerabilities such as a configuration error that grants file access to all users, or makes use of "trapdoors" originally inserted by system developers for system maintenance.

3. **Network spoofing**, in which the hacker's system impersonates another system when attempting to log on to a network.

D. Safeguards

Sections H through K chart four categories of safeguards against the threats posed by malicious software and intrusions. The categories include technical controls, software management, contingency planning, and system monitoring/intrusion detection. Each of these tables contains examples of safeguards that can be used for computers of all sizes.

E. User Security Awareness Training

Section L charts subjects that can be addressed in elevating user awareness about malicious software and intrusions. Users must understand what is expected of them and what activities are violations of policy, such as loading unapproved software on their microcomputers or using systems and data for which they are not authorized. They must be instructed in how to use the system safeguards that protect systems and data. Adequate user awareness training can go a long way toward preventing the effects of malicious software and hackers.

F. Sign-On Warning

In conjunction with a review of the legal propriety of keystroke monitoring, the Department of Justice (DOJ) has advised the National Institute of Standards and Technology (NIST) that government agencies should warn system users that, by using a system, they are expressly consenting to keystroke monitoring. Provision of written notice in advance to only authorized users is not sufficient. Since it is important that unauthorized intruders be given notice, some form of banner notice at the time of signing on to the system is required.

An agency's banner should give clear and unequivocal notice to intruders that by signing on to the system they are expressly consenting to such monitoring. The banner should also indicate to authorized users that they may be monitored during an effort to monitor an intruder (e.g., if a hacker is downloading a user's file, keystroke monitoring will intercept both the hacker's download command and the authorized user's file). In addition, system administrators may monitor authorized users in the course of routine system maintenance.

DOJ and NIST have provided the following example of an appropriate banner. It is the only official guidance available at the time of publication of this Handbook regarding sign-on warnings:

This system is for the use of authorized users only. Individuals using this computer system without authority, or in excess of their authority, are subject to having all of their activities on this system monitored and recorded by system personnel. In the course of monitoring individuals improperly using this system, or in the course of system maintenance, the activities of authorized users may also be monitored. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence of such monitoring to law enforcement officials.

No specific language is required at this time, and Agencies are encouraged to tailor the banner to their precise needs. For example, the banner might contain a statement concerning the need to protect private data from unauthorized disclosure (e.g., *"The Privacy Act of 1974 states that all private data must be protected from unauthorized disclosure. Anyone reading this data is responsible for the privacy of data displayed on a computer monitor/CRT or printed in a report."*). An agency may also want to consider mentioning the legal penalties to an individual who signs on to a Federal system without authorization.

G. Computer Security Incident Response Capabilities (CSIRC)

Computer systems and communication networks are subject to a variety of sophisticated threats. Malicious software, in particular, is a large and growing threat that can cause enormous harm in a short period of time. Prevention, by the use of anti-virus software must be the main line of defense. When a security incident occurs there is a need to respond quickly with on-call expertise that can control and contain sophisticated intrusions, limit damage, eliminate the problem, and restore normal operations.

Currently most problems of an immediate nature are dealt with by contacting the ISM Headquarters Computer Support Center to discuss the problem with knowledgeable peers. Most problems involving hardware, software and procedures are effectively resolved in making this call for assistance.

A CSIRC is a part of the computer security effort that provides the capability to respond to computer Security threats rapidly and effectively. The FedCIRC provides the means for the Federal agencies, law enforcement, private sector, and academia to work together to handle IT Security incidents, share related information, solve common IT security problems, and plan future IT Infrastructure protection strategies. A CSIRC provides a way for users to report incidents, and it provides personnel and tools for investigating and resolving incidents, and mechanisms for disseminating important incident-related information to management and users. The Department of the Interior currently has a Letter of Agreement with The Federal Computer Incident Response Capability to provide this direct assistance.

1. **CSIRC components:**

a. The OSM Point of Contact, is the ISSO (202) 208-2910, or page at (202) 319-2013, (CSIRC Coordinator ISM,) is responsible for follow-up reporting and issues clarification.

b. The FedCIRC Management Center POC can be contacted at (202) 708-7201 (Computer Emergency Response Team).

c. The FedCIRC Operations Center (Carnegie Mellon University Software Engineering Institute) POC can be contacted at (888) 282-0870.

d. Communication is maintained with the FedCERC facilities and the DOI user community.

e. A contact list is used to facilitate rapid communication.

2. **Steps to dealing with CSIRC:**

a. Contact ISM Headquarters Support Center, if possible, as a first step.

b. Contact other DOI POC for assistance if appropriate.

c. Contact FedCERC facilities at any time if you wish to report, access information or need assistance on a incident response action.

d. Report all IT security incidents to the ISSO.

H. Technical Controls

Password Management	Require effective passwords for all logons.
	Eliminate easily guessed passwords, including all proper names and dictionary words.
	Make password files inaccessible.
	Schedule regular password changes.
	Accept only a limited number of password attempts before disabling an account.
File Access Management	Set default access for all files to owner-only.
	Provide access only to programs and users who require access.
	Provide only read access unless write access is required.
	Review access permissions periodically.
Microcomputer Accessibility	Reduce microcomputer accessibility by: Removing floppy disk drives or using diskless computers. Using commercial software to provide password protection. Using add-on hardware for user authentication.

I. Software Management

System Software	Stay abreast of known operating system vulnerabilities and specific fixes (Service packs and fixes).
	Use current versions of all operating systems.
	Prevent user access to system software and data.
	Identify and eliminate or change any "trapdoors" inserted by system developers.
User Software	Prohibit users from installing software directly.
	Develop a mechanism, such as virus scanning, for validating software (particularly public domain software) before installation.
	Only install software (e.g., compiler or debugger) that is clearly needed on user machines.
	Prohibit users from adding software to LAN software repositories.
	Maintain a database of all installed user software for quick location of suspect software.

J. Contingency Planning

Backups	Write-protect application software diskettes.
	Back up and safe-store application software.
	Restore software only from its original medium, rather than from backup tapes/disks.
	Follow a regular schedule for data backup.
Incident Response	Develop a Computer Security Incident Response Capability (CSIRC). (See Chapter VI, "Contingency Planning.")

K. System Monitoring/Intrusion Detection

Tools	Use virus scanners for routine checks of all microcomputer and LAN software.
	Use system audit tools to monitor accesses to accounts and files.
	Use system sweep programs to checksum files and report differences.
Procedures	Review monitor tool logs regularly.
	Investigate all suspicious activities.
	Enforce sanctions against users who consistently violate security policies.

L. Necessary User Awareness Training

Malicious Software and Intrusions	Methods of operation and transfer of malicious software; nature of intrusions
	Vulnerabilities exploited by malicious software and hackers
	Security and productivity consequences
Safeguards	Security policies and procedures
	Recognition of abnormal system activity
	Role of CSIRC

Chapter XIII. – Access Controls

A. Overview

This chapter establishes policies and procedures designed to safeguard information systems and data by establishing system access controls. All personnel will adhere to the following requirements classified as LAN Administration, Personnel Practices, Access Rights, Custodial, Telecommunication, Evaluation and General.

B. LAN/System Administration Requirements

Administrators will implement technical controls necessary to ensure that the threat to powerful network operating system commands by unauthorized individuals is minimized. Inappropriate control over these commands could allow unauthorized users to gain control over network resources. Examples of these commands in a Novell operating environment include 'Secure Console', 'Lock Console' and 'Rconsole'. The Administrators will ensure that all steps have been taken to minimize the inappropriate use of these commands by unauthorized individuals. The following must be ensured:

1. The user-ID will be unique to each user and will identify the user to the system. The assignment of more than one user or a phantom user to a user-ID is prohibited.

2. Whenever possible, passwords will be user generated under the supervision of access control software. In facilities where access control software is not available, the IT Specialist/System Manager will create and distribute user passwords in a controlled manner, and in such a way that an audit record of password date and time of issuance, receipt, use, change, expiration and termination is maintained.

3. System users will gain access to networks or distributed systems only after entering their unique user-ID and a password.

4. Passwords will be valid for a period of not more than 90 days.

5. System users will not share their system passwords with anyone, even another cleared user.

6. System Administrators must activate the audit trail capabilities provided by the operating system and security software installed on Agency systems.

7. System Administrators will manage the creation, use and deletion of user IDs and password to prevent unauthorized access to the system. This process will ensure that employee terminations, transfers, or re-assignments of

responsibilities result in a subsequent assessment of the need for user accounts and associated user rights to files and systems. This process will be carried out in a uniform and consistent manner throughout OSM, and will be achieved in concert with standard operating procedures of the Office of Personnel for Federal employees and individual Contracting Officer Technical Representatives for contract employees.

8. The SISSO must ensure all system users are aware of the private nature of their passwords. Users must inform the Administrator if they suspect their password has been compromised.

9. ISSO and System Managers will ensure that Administrators log onto information systems under specific user ID's designated for system administration purposes.

10. Password file maintenance will be restricted to the LAN Managers and System Administrators, and passwords will be screen-suppressed during logon and re-authentication.

11. Users will be required to use passwords randomly selected and consisting of a combination of at least six alpha, numeric or special characters that cannot be traced back to the user (recognizable words, phrases, or dates must not be used).

12. When the password expires, the operating system or security software must prompt the user to change passwords.

13 An audit trail will be implemented and viewed periodically and will record at least the following events and any other events deemed appropriate by the Responsible Official:

a. Multiple logon failures;

b. Logons during non-business hours;

c. Addition, deletion, or modification of user or program access privileges; and

d. Changes in file access restrictions.

14. System Administrator must archive the audit trail to a file with the most stringent access restrictions available. Audit trails containing financial information and transactions must be retained for a period of two years. Audit trails containing information not related to financial information and transactions must be retained for an appropriate time period.

15. The System Administrator will not maintain permanent user-IDs and

passwords on computer systems for visitors, vendor service personnel, training, or demonstrations.

16. The System Administrator will delete all default user-IDs and passwords supplied by the vendor during system manufacture and installation once installation is complete.

17. The System Administrator must cause all system users to change their passwords under the following conditions: at least every 90 days (30 days for dial-in access); immediately following any suspected compromise; and whenever there are changes in personnel with system security authority.

18. The System Administrator must immediately delete user-IDs and passwords whenever the Supervisor determines that the user no longer requires system access. (See Chapter I Paragraph E, 13e)

19. Use of information systems equipment owned or operated by the Agency for purposes other than authorized U.S. Government use is prohibited.

20. Logged on workstations are not left unattended unless locked or password protected. However, employees will not engage or set Basic Input Output System (BIOS) password access controls on individual PCs.

21. After-Hour System Operation

a. The Site ISSO and System Managers must ensure appropriate after-hour restrictions are developed and implemented for each system under their purview.

b. The System Manager must ensure all system logs in effect during normal operations are also activated during after-hour operations.

22. Protection of Media and Output - The System Manager must store back-up copies of operating system and application software, in an authorized off-site locked area or approved security container.

C. Personnel Practices Requirements

Only individuals who meet the requirements for sensitive systems and related automated data processing positions (those with proper clearances) will be users with special access privileges.

D. Access Rights Requirements

Program Managers are responsible for ensuring separation of duties and implementing controls to prevent fraud, waste and abuse.

1. Accordingly, the System Manager, or System Owner as appropriate, must structure user access privileges to reflect the separation of key duties implemented for functions supported by the application. All user access privileges must be consistent with the separation of duties established for manual processes and be reviewed on an annual basis.

2. The System Manager, or System Owner as appropriate, must revoke the user access privileges of personnel no longer requiring system access or personnel that have severed their relationship with the Agency. Such revocation must take place immediately upon the employee's status change or departure.

3. The System Manager, or System Owner as appropriate, must implement all application controls to ensure users are assigned access rights and privileges consistent with their functional responsibilities and authorities. Access rights and privileges must be based on need-to-know, separation of duties, and management authorization. This will include assurances that public users do not have inappropriate access to computer resources. It must also ensure that only authorized users have 'root' access.

4. The System Administrator must ensure necessary security controls are implemented to prevent unauthorized access to OSM systems. The System Administrator will ensure that the following restrictions are enforced:

a. The LAN, or host computer systems, disconnects a logged on client workstation or microcomputer from the system after a predetermined period of inactivity.

b. Limit unsuccessful logon attempts from any user account to three. After three unsuccessful logon attempts, the system will automatically lock out the user account. Only the System Administrator will be given the capability to reset a user account after lockout.

c. Any systems that cannot be set to three unsuccessful login attempts will be set to the minimum possible.

d. System Manager, or System Owner as appropriate, will formally assign responsibility for approving systems access to appropriate personnel.

e. Controls are implemented which limits access to files, programs, and data to users or groups of users with the same need-to-know. Need-to-know shall be based on functional responsibilities, operational requirements, supervisory responsibilities, or a combination of these factors.

f. The System Administrator with the help of the SISSO is to ensure that all security updates and patches are evaluated and approved as appropriate.

g. All security software that was provided as part of the original system configuration (e.g., audit trail) is installed and operational.

h. Each system user is assigned a valid and appropriate logon procedure to control the processing options available to the system user.

E. Custodial Requirements

The Program Managers will ensure unauthorized custodial and building maintenance personnel entering areas designated as a Sensitive Computer Area (SCA), are under continual observation by personnel with authorized unescorted access. [NOTE: The SISSO is responsible for identifying all SCAs within his jurisdiction. Typically, an SCA would include those areas where servers, routers, or other networking hardware devices are put into operation.]

1. The SISSO will develop and maintain a list of personnel who will be granted unescorted access into the SCA.

2. The SISSO must maintain a visitors' log for all persons entering the SCA who do not have unescorted access privileges. Only personnel listed on the "Authorized Access List" will escort visitors. Individuals not on the "Authorized Access List" must sign the visitors' log prior to being allowed access into the SCA. While in the SCA, visitors must be under continuous visual observation by a person with authorized unescorted access.

F. Telecommunication Requirements

Users will not physically connect via modem, Internet service providers, or other means, personally owned microcomputers or communication devices to U.S. Government owned systems or communication devices within OSM facilities, without the prior authorization of the system administrator. It is understood that authorization for connection may be granted if said connectivity is necessary for systems or applications development testing.

1. Bureau employees and/or users having system accounts will not physically connect via modem, Internet service providers, or other means to government owned computers, workstations, servers, routers or any other computing or telecommunication devices without the prior written authorization from appropriate LAN administrators or system administrators responsible for the system. The LAN or System administrator may grant a temporary exception if said connectivity is necessary for official systems or applications development requiring testing of telecommunication

capabilities. This authorization will be of a temporary nature, and once tested, the restriction against outside connectivity will be put back in place.

2. Bureau employees and/or users having system accounts may not automatically forward e-mail from Government e-mail systems to personal or remote systems without the express written authorization of the LAN administrator. Message forwarding of this type might be used to inadvertently telecommunicate secure or sensitive government data to an insecure or inappropriate location.

3. Bureau employees and/or users having system accounts may not set up remote access capabilities to control or monitor government computers from remote locations (unless said remote locations are at authorized government offices) without the express written authorization of LAN or system administrators. Failure to follow this procedure could result in compromise by an insecure telecommunications connection. For example, an employee of the Bureau may not run a PC-anywhere type of application from his or her office computer that would accept a connection from the employee's home computer, without the express written authorization of the LAN or system administrator. The LAN or system administrator is authorized to grant a connection of this nature only after performing a review of the need and assessment of security measures in place.

G. Evaluation Requirements

The Information Security Officers Review Team (iSORT) will periodically evaluate capabilities, and, where necessary, implement procedures, to address state of the art encryption techniques to help ensure the integrity of system level passwords when transmitted over the network.

System Owners must periodically review the access privileges of each application user under their jurisdiction to verify system access privileges originally granted are still appropriate.

H. Software and Applications Requirements

1. The Program Manager will ensure that only OSM approved or distributed versions of customized agency or corporate application software (microcomputer software excluded) are used on computer systems and networks owned or operated by OSM.

2. Authorized application developers are the only personnel authorized to modify OSM standard application software.

3. Employees developing application software for OSM systems, will develop and document their application software in accordance with industry standards and practices.

4. The Supervisor will ensure that personally owned software, shareware or freeware are not installed on computer systems owned or operated by OSM without the approval of the Supervisor and IT support.

5. All software must be scanned for viruses and other malicious programming code prior to installation on any computer system or network owned or operated by the OSM. Virus scanning software will be installed on all workstations and microcomputers in the OSM.

Appendix A1. Information Systems Security Quick Reference Guide

Minimum Security Requirements	Act 1987*	A-130	A-123 A-127	CFR	FIRMR	PA/FOIA	NIST Pubs
Program Responsibilities Implement and maintain ISSP; assign responsibilities.		X			X	X	
Security Plans Identify sensitive systems; implement security plans.	X				X		800-18
Applications Security Review applications systems every 3 years. Develop and maintain contingency plans.		X X	X		X X		73, 102 87
Installation Security Conduct risk analysis every 5 years. Prepare acquisition specifications. Maintain disaster recovery plans.		X X X	X		X X X		31, 65 87
Personnel Security Designate all positions and screen incumbents.		X		X	X		
Security Awareness and Training Train Federal and contractor personnel.	X	X					500-172
Reporting Report security weaknesses in A-123 Report to President.		X	X				

Appendix A2. Reference Detail Listings

A. Public Policy and Law

Computer Crime Act of 1984.

Computer Security Act of 1987, P.L. 100-235 (1988).

Concealment, Removal, or Mutilation Generally, 18 U.S.C. 1071 (1948).

Disclosure of Confidential Information Generally, 18 U.S.C. 1905 (1948).

Federal Manager's Financial Integrity Act of 1982, P.L. 97-255, 31 U.S.C. 66a (1982).

Interception and Disclosure of Wire or Oral Communications Prohibited, 18 U.S.C. 2511 (1968).

Malicious Mischief, 18 U.S.C. 1361 (1967).

Paperwork Reduction Act of 1980, P.L. 96-511, 44 U.S.C. 3501-3520 (1980), as amended in the Paperwork Reauthorization Act.

Privacy Act of 1974, P.L. 93-579, 5 U.S.C. 552a (1974).

Public Money, Property, or Records, 18 U.S.C. 641 (1948).

B. Office of Management and Budget

OMB Circular A-11, "Preparation and Submission of Budget Estimates," June 17, 1988.

OMB Circular A-109, "Major Systems Acquisitions," April 5, 1976.

OMB Circular A-123, Revised, "Internal Control Systems," August 4, 1986.

OMB Circular A-127, "Financial Management Systems," December 19, 1984.

OMB Circular A-130, "Management of Federal Information Resources," December 12, 1985.

OMB Bulletin No. 90-08, "Guidance for Preparation of Security Plans for Federal Computer Systems that Contain Sensitive Information," July 9, 1990.

OMB *Internal Control Guidelines*, December 1982.

"OMB Revised Supplemental Guidance for Conducting Computer Matching Programs," FR 47, 21656-21658, May 19, 1982.

C. General Accounting Office

Executive Guide, Information Security Management, May 1998

D. General Services Administration

Federal Information Resources Management Regulation (FIRMR), 1990.

Federal Procurement Management Regulations.

GSA Handbook, "Federal ADP and Telecommunications Standards Index."

FIRMR Bulletin C-22, "Security and Privacy Protection of Federal Information Processing (FIP) Resources," September 18, 1992.

FIRMR Bulletin C-28, "Computer Viruses," November 6, 1990.

41 *Code of Federal Regulations* (CFR) Subparts 1-4.11, "Procurement and Contracting Government-wide for Automated Data Processing, Equipment, Software, Maintenance Services, and Supplies."

E. Office of Personnel Management

5 CFR 731 "Suitability."

5 CFR 732, "National Security Positions."

5 CFR 736 "Personnel Investigations"

5 CFR Part 930, "Training Requirements for the Computer Security Act."

36 CFR Part 1234 "Electronic Records Management"

F. National Institute of Standards and Technology

CSC_STD-003-85, "Guidance For Applying The Bureau Of Defense Trusted Computer System Evaluation Criteria In Specific Environments," June 25, 1985.

DOD 52200.28 STD, "Trusted Computer Systems Evaluation Criteria," December 1985.

Federal Information Processing Standards Publication (FIPS) 11-3, *American National Dictionary for Information Systems*, February 1991.

FIPS PUB 31, *Guidelines for Automated Data Processing Physical Security and Risk Management*, June 1974.

FIPS PUB 38, *Guidelines for Documentation of Computer Programs and Automated Data Systems*, February 1976.

FIPS PUB 41, *Computer security Guidelines for Implementing the Privacy Act of 1974*, May 1975.

FIPS PUB 46-1, *Data Encryption Standard*, January 1988.

FIPS PUB 48, *Guidelines on Evaluation Techniques for Automated Personnel Identification*, April 1977.

FIPS PUB 64, *Guidelines for Documentation of Computer Programs and Automated Data Systems for the Initiation Phase*, August 1979.

FIPS PUB 65, *Guideline for Automated Data Processing Risk Analysis*, August 1979.

FIPS PUB 73, *Guidelines for Security of Computer Applications*, June 1980.

FIPS PUB 74, *Guidelines for Implementing and Using the NBS Data Encryption Standard*, April 1981.

FIPS PUB 81, *DES Modes of Operation*, December 1980.

FIPS PUB 83, *Guideline on User Authentication Techniques for Computer Network Access Control*, September 1980.

FIPS PUB 87, *Guidelines for ADP Contingency Planning*, March 1981.

FIPS PUB 88, *Guideline on Integrity Assurance and Control in Database Administration*, August 1981.

FIPS PUB 101, *Guideline for Lifecycle Validation, Verification, and Testing of Computer Software*, June 1983.

FIPS PUB 102, *Guideline for Computer Security Certification and Accreditation*, September 1983.

FIPS PUB 112, *Password Usage*, May 1985.

FIPS PUB 113, *Computer Data Authentication*, May 1985.

FIPS PUB 132, *Guideline for Software Verification and Validation Plans*, November 1987.

FIPS PUB 139, *Interoperability and Security Requirements for Use of the Data Encryption Standard in the Physical Layer of Data Communications*, August 1983.

FIPS PUB 140, *General Security Requirements for Equipment Using the Data Encryption Standard*, April 1982.

FIPS PUB 141, *Interoperability and security Requirements for Use of the Data Encryption Standard with CCIT Group 3 Facsimile Equipment*, April 1985.

FIPS PUB 146-1, *Government Open Systems Interconnection Profile (GOSIP)*, April 1991.

FIPS PUB 171, *Key Management Using X9.17*, April 1992.

FIPS PUB 180, *Secure Hash Standard*, May 1993.

FIPS PUB 181-1, *Digital Signature Standards (DSS)*, December 1998.

FIPS PUB 191, *Guidelines for the Analysis of Local Area Network Security*, November 1994.

FIPS PUB 196, *Entity Authentication Using Public Key Cryptography*, February 1997.

Special Publication (SPEC PUB) 500-109, *Overview of Computer security Certification and Accreditation*, April 1984.

SPEC PUB 500-120, *Security of Personal Computer Systems: A Management Guide*, January 1985.

SPEC PUB 500-133, *Technology Assessment: Methods for Measuring the Level of Computer Security*, October 1985.

SPEC PUB 500-134, *Guide on Selecting ADP Backup Process Alternatives*, November 1985.

SPEC PUB 500-136, *An Overview of Computer Software Acceptance Testing*, February 1986.

SPEC PUB 500-137, *Security for Dial-Up Lines*, May 1986.

SPEC PUB 500-153, *Guide to Auditing for Controls and security: A System Development Life Cycle Approach*, April 1988.

SPEC PUB 500-157, *Smart Card Technology: New Methods for Computer Access Control*, September 1988.

SPEC PUB 500-161, *Software Configuration Management: An Overview*, March 1989.

SPEC PUB 500-166, *Computer Viruses and Related Threats: A Management Guide*, August 1989.

SPEC PUB 500-169, *Executive Guide to the Protection of Information Resources*, October 1989.

SPEC PUB 500-170, *Management Guide to the Protection of Information Resources*, October 1989.

SPEC PUB 500-171, *Computer User's Guide to the Protection of Information Resources*, October 1989.

SPEC PUB 500-173, *Guide to Data Administration*, October 1989.

SPEC PUB 500-174, *Guide to Selecting Automated Risk Analysis Tools*, October 1989.

SPEC PUB 500-180, *Guide to Software Acceptance*, April 1990.

SPEC PUB 800-3, *Establishing a Computer Security Incident Response Capability* (CSIRC), November 1991.

SPEC PUB 800-4, *Computer Security Considerations in Federal Procurements: A Guide for Procurement Initiators, Contracting Officers, and Computer Security Officials*, March 1992.

SPEC PUB 800-5, *A Guide to the Selection of Anti-Virus Tools and Techniques*, December 1992.

SPEC PUB 800-6, *Automated Tools for Testing Computer System Vulnerability*, December 1992.

SPEC PUB 800-7, *Security In Open Systems*, July 1994.

SPEC PUB 800-10, *Keeping Your Site Comfortably Secure: An Introduction to Internet Firewalls*, December 1994.

SPEC PUB, 800-12, *An Introduction to Computer Security: The NIST Handbook*, October 1995.

SPEC PUB, 800-13, *Telecommunications Security Guidelines for Telecommunications Management Networks,* October 1995.

SPEC PUB 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems,* June 1996.

SPEC PUB 800-16, *Information Technology Security Training Requirements: A Role and Performance Based Model,* March 1998.

SPEC PUB 800-18, *Guide for Developing Security Plans for Information Technology Systems,* December 1998.

NISTIR 4636, *U.S. Dept. of Health and Human Services (HHS) Information Systems Security Handbook*, July 1991.

NISTIR 4659, *Glossary of Computer Security Terminology*, September 1991.

NISTIR 4749, *Sample Statements of Work for Federal Computer Security Services: For Use In-House or Contracting Out*, December 1991.

NISTIR 4846, *Computer Security Training & Awareness Course Compendium*, May 1992.

NISTIR 4939, *Threat Assessment of Malicious Code and External Attacks*, October 1992.

NISTIR 4976, *Assessing Federal and Commercial Information Security Needs*, November 1992.

NISTIR 5153, *Minimum security Requirements for Multi-User Operating Systems*, March 1993.

NIST Publication List 58, *FIPS PUBS Index.*

NIST Publication List 88, *Computer Systems Publications.*

NIST Publications List 91, *Computer Security Publications.*

G. National Telecommunication and Information Systems Security

NTISS Directive 900 "Governing Procedures Of The National Telecommunication And Information Systems Security (NTISS) Committee," March 1, 1985, and subsequent directives and guidelines to be issued by NTISS Committee.

H. Office of Surface Mining Reclamation and Enforcement

Information Systems Life Cycle Guidance, INF-11

Computer Users Guidance Manual, June 1999

I. DOI

375 DM 19, *DOI Security Manual.*

441 DM 1-6, *Personnel Suitability and Security Investigation Requirements*

444 DM 1, *Physical Protection and Building Security.*

442 DM 1-15, *National Security Information*

J. Other

Department Of Commerce, RP-1, *Standard Practice For The Fire Protection Of Essential Electronic Equipment Operations,* 1978

Department of Commerce, RP-1, *Standard Practice for the Fire Protection of Essential Electronic Equipment Operations,* 1978.

Lawrence Livermore National Laboratory UCRL-ID-104689, *Responding to Computer Security Incidents: Guidelines for Incident Handling*, July 1990.

Microsoft Press Computer Dictionary: The Comprehensive *Standard for Business, School, Library, and Home*. Redmond, WA: Microsoft Press, 1991.

NFPA, Publication 75-1992, *Protection of Electronic Computer/Data Processing Equipment*, 1992.

NISTIR 4659, *Glossary of Computer Security Terminology,* September 1991.

President's Council on Management Improvement and the President's Council on Integrity and Efficiency, *Model Framework for Management Control Over Automated Information Systems.* Washington, DC: GPO, 1988.

Appendix B. Definitions

ACCESS TO INFORMATION Access to information refers to the function of providing to members of the public, upon their request, the Government information to which they are entitled under law. (OMB Circular A-130)

APPLICATION SYSTEM An application system is a computer system written by or for a user that applies to the user's work; for example, a payroll system, inventory control system, or a statistical analysis system. (FIPS PUB 11-3)

APPLICATION SYSTEM MANAGER An Application System Manager is the official who is responsible for the operation and use of an application system. (OSM Definition)

COMPUTER SECURITY INCIDENT RESPONSE CAPABILITY (CSIRC) A CSIRC is that part of the computer security effort that provides the capability to respond to computer security threats rapidly and effectively. [A CSIRC provides a way for users to report incidents, and it provides personnel and tools for investigating and resolving incidents, and mechanisms for disseminating incident-related information to management and users. Analysis of incidents also reveals vulnerabilities, which can be eliminated to prevent future incidents.] (NIST SPEC PUB 800-3)

COMPUTER SYSTEM Any equipment or interconnected system or subsystems of equipment used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information; including computers; ancillary equipment; software, firmware, and similar procedures; services, including support services; and related resources as defined by regulations issued by the Administrator for General Services pursuant to section 111 of the Federal Property and Administrative Services Act of 1949. (Computer Security Act of 1987)

COMPUTER SYSTEMS SECURITY PLAN (CSSP) The CSSP provides a basic overview of the security and privacy requirements of the subject system and the agency's plan for meeting those requirements. (OMB Bulletin 90-08)

CONTINGENCY PLAN A contingency plan is a plan for emergency response, backup procedures, and post-disaster recovery. Synonymous with disaster plan and emergency plan. (FIPS PUB 11-3)

DATA COMMUNICATIONS Data communication is the transfer of data between functional units by means of data transmission according to a protocol. (FIPS PUB 11-3)

DATABASE A database is a collection of interrelated data, often with controlled redundancy, organized according to a schema to serve one or more applications; the data are stored so that different programs without concern for the data structure or organization can use them. A common approach is used to add new data and to modify and retrieve existing data. (FIPS PUB 11-3)

DATABASE MANAGER A Database Manager is the official who is responsible for the operation and use of a database. (OSM Definition)

DISSEMINATION OF INFORMATION Dissemination of information refers to the function of distributing Government information to the public, whether through printed documents, or electronic or other media. Dissemination of information does not include intra-agency use of information, inter-agency sharing of information, or responding to public requests for access to information. (OMB Circular A-130)

FEDERAL COMPUTER SYSTEM A Federal computer system is a computer system operated by a Federal agency or by a contractor of a Federal agency or other organization that processes information (using a computer system) on behalf of the Federal Government to accomplish a Federal function. A Federal computer system includes automatic data processing equipment as that term is defined in section 111(a)(2) of the Federal Property and Administrative Services Act of 1949. (Computer Security Act of 1987)

GOVERNMENT INFORMATION Government information is any information that is created, collected, processed, transmitted, disseminated, used, stored, or disposed of by the Federal Government. (OMB Circular A-130)

INFORMATION Information is any communication or reception of knowledge, such as facts, data, or opinions, including numerical, graphic, or narrative forms, whether oral or maintained in any other medium, including computerized databases, paper, microform, or magnetic tape. (OMB Circular A-130)

INFORMATION SYSTEM (IS) An IS is the organized collection, processing, transmission, and dissemination of automated information in accordance with defined procedures. (OMB Circular A-130)

INFORMATION RESOURCES MANAGEMENT (IRM) IRM is the planning, budgeting, organizing, directing, training, and control associated with Government information. The term encompasses both the information itself and related resources, such as personnel, equipment, funds, and technology. (OMB Circular A-130)

INFORMATION SYSTEM SECURITY [COMPUTER SECURITY] Information system security refers to the concepts, techniques, technical measures, and administrative measures used to protect the hardware, software, and data of an information processing system from deliberate or inadvertent unauthorized acquisition, damage, destruction, disclosure, manipulation, modification, use, or loss. (FIPS PUB 11-3)

INFORMATION SYSTEMS SECURITY (INFOSEC) An INFOSEC is the protection afforded to information systems to preserve the availability, integrity, and confidentiality of the systems and information contained in the systems. [Protection results from the application of a combination of security measures, including crypto-security, transmission security, emission security, computer security, information security, personnel security, resource security, and physical security.] (NISTIR 4659)

INFORMATION TECHNOLOGY FACILITY An information technology facility is an organizationally defined set of personnel, hardware, software, and physical facilities, a primary function of which is the operation of information technology. [Information technology facilities range from large centralized computer centers to individual stand-alone microcomputers.] (OMB Circular A-130)

MALICIOUS SOFTWARE Malicious software is the collective name for a class of programs intended to disrupt or harm systems and networks. The most widely known example of malicious software is the computer virus; other examples are Trojan horses and worms. (OSM Definition, adapted from NIST SPEC PUB 500-166)

PERSONNEL SECURITY Personnel security refers to the procedures established to ensure that each individual has a background which indicates a level of assurance of trustworthiness which is commensurate with the value of information technology resources which the individual will be able to access. (NISTIR 4659)

PHYSICAL SECURITY Physical security refers to the application of physical barriers and control procedures as preventive measures and countermeasures against threats to resources and sensitive information. (NISTIR 4659)

RISK ASSESSMENT A risk assessment is the identification and study of the vulnerability of a system and the possible threats to its security. (FIPS PUB 11-3)

RISK MANAGEMENT Risk management is the process of identifying, controlling, and eliminating or minimizing uncertain events that may affect system resources. It includes risk analysis, cost benefit analysis, selection, implementation and test, security evaluation of safeguards, and overall security review. (NISTIR 4659)

SENSITIVE APPLICATION A sensitive application is an application of information technology that requires protection because it processes sensitive data, or because of the risk and magnitude of loss or harm that could result from improper operation, deliberate manipulation, [or delivery interruption] of the application. (OMB Circular A-130)

SENSITIVE COMPUTER AREA (SCA) Would include those areas where servers, routers or other networking devices are put into operation.

SENSITIVE DATA Sensitive data are data that require protection due to the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the data. The term includes data whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary data, records about individuals requiring protection under the Privacy Act, and data not releasable under the Freedom of Information Act. (OMB Circular A-130)

SENSITIVE INFORMATION Sensitive information is any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect OSM.

SIGNIFICANT CHANGE A significant change is a physical, administrative, or technical modification that alters the degree of protection required. Examples include adding a local area network, changing from batch to on-line processing, adding dial-up capability, and increasing the equipment capacity of the installation. (OSM Definition)

USER A user is any organizational or programmatic entity that [utilizes or] receives service from an [automated information system] facility. A user may be either internal or external to the agency organization responsible for the facility, but normally does not report to either the manager or director of the facility or to the same immediate supervisor. (OMB Circular A-130)

Appendix C. Acronyms

ANACI	Access National Agency Check and Inquires Investigation
BI	Background Investigation
CERTeam	Computer Emergency Response Team
COTR	Contracting Office Technical Representative
CSIRC	Computer Security Incident Response Capability
CSSP	Computer Systems Security Plan
DCIO	Deputy Chief Information Office for Information Resources Management
FedCIRC	Federal Computer Incident Response Center
FIPS PUB	Federal Information Processing Standards Publication
FIRMR	Federal Information Resources Management Regulation
FPPS	Federal Personnel Processing System
ICR	Internal Controls Review
IS	Information Systems
iSORT	Information Security Officer Review Team
ISSO	Information Systems Security Office
ISSP	Information Systems Security Program
IT	Information Technology
NACI	National Agency Check and Inquiries Investigation
NACIC	National Agency Check and Inquiries plus Credit Check Investigation
NACLC	National Agency Check with Law and Credit Investigation
NARA	National Archives and Records Administration
NFPA	National Fire Protection Association
NIST	National Institute of Standards and Technology
NSS	Network System Support, at Headquarters
PM	Program Managers
SISSO	Site Information Systems Security Officer
SSBI	Single Scope Background Investigation
SPEC PUB	(NIST) Special Publication