NISTIR 4636

U.S. Department of Health and Human Services'

Automated Information Systems Security Program Handbook

Edward Roback
NIST Coordinator

U.S. DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
Gaithersburg, MD 20899

U.S. DEPARTMENT OF COMMERCE
Robert A. Mosbacher, Secretary
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
John W. Lyons, Director

NIST

NISTIR 4636

U.S. Department of Health and Human Services'

Automated Information Systems Security Program Handbook

Edward Roback
NIST Coordinator

U.S. DEPARTMENT OF COMMERCE
National Institute of Standards
and Technology
Gaithersburg, MD 20899

July 1991

U.S. DEPARTMENT OF COMMERCE
Robert A. Mosbacher, Secretary
NATIONAL INSTITUTE OF STANDARDS
AND TECHNOLOGY
John W. Lyons, Director

Preface

This National Institute of Standards and Technology Interagency Report (NISTIR) presents the U.S. Department of Health and Human Services' (HHS) Automated Information Systems Security Program Handbook. The Handbook provides a comprehensive description of the program elements which comprise HHS' approach to computer security. Among the varied items included are: security policy and responsibilities, security level designators, security level requirements, security administration, risk management, contingency planning, personnel security, facility security, application systems and data security, personal computers, data communications, and acquisitions and contracts.

The National Institute of Standards and Technology (NIST) makes no claim or endorsement of this Handbook. However, as this material may be of use to other organizations, the report is being reprinted by NIST to provide for broad public dissemination of this federally sponsored work. This publication is part of a continuing effort to assist federal agencies in accordance with NIST's mandate under the Computer Security Act of 1987.

NIST expresses its appreciation to the Office of the Secretary at HHS their kind permission to publish this report.

Questions regarding this publication should be addressed to the Associate Director for Computer Security, Computer Systems Laboratory, Building 225, Room B154, National Institute of Standards and Technology, Gaithersburg, MD, 20899.

Additional copies of this publication may be purchased through the National Technical Information Service, Springfield, VA, 22161, telephone: (703) 487-4650.

Automated Information Systems Security Program Handbook

(Release 1.0)

Department of Health and Human Services

TABLE OF CONTENTS

Appendices

Exhibit

CHAPTER I. AIS SECURITY PROGRAM

A. OVERVIEW

The Department of Health and Human Services (DHHS) is responsible for implementing and administering a program to protect its information resources. The program must comply 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. In compliance with these requirements, the Department has instituted the Automated Information Systems (AIS) Security Program. The AIS Security Program applies to all DHHS organizations and their employees, including agents (e.g., contractors) of DHHS, who are responsible for the acquisition, management, and/or use of information resources in both hard copy and electronic form.

The Department's AIS Security Program has three basic documents. DHHS IRM Circular, Automated Information Systems Security Program establishes policies, procedures, and responsibilities for the implementation and administration of the AIS Security Program. This Handbook contains the security procedures and guidance for the Department. The AIS Security Training and Orientation Program Guide for the Department contains procedural guidance for implementing security awareness and training.

The purpose of this chapter is to provide an overview of this Handbook. This chapter includes the Department's AIS security policy, a listing of security responsibilities, an overview of AISSP content, and summaries of all subsequent chapters in this Handbook. It should be noted that many of the responsibilities are re-listed in the chapters. The reason for this duplication is simply to allow each chapter to be as free-standing as possible.

B. AIS SECURITY POLICY

DHHS will implement a Department-wide AIS security program to assure that each automated 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:

a. each AIS have the appropriate technical, personnel, administrative, environmental, and telecommunications safeguards;

b. AIS security should be cost-effective; and

c. an AIS which supports critical OPDIV functions has a contingency or disaster recovery plan to provide continuity of operation.

Each OPDIV shall administer an AIS security program that meets statutory, regulatory, and Departmental requirements and the needs of the OPDIV and the public.[1]

C. AIS SECURITY PROGRAM CONTENT

In accordance with overall DHHS policy, the AISSP established by the Operating Divisions/Staff Divisions (OPDIVs/STAFFDIVs) and Regional Offices (ROs) must fulfill the following minimum requirements:

Policy

1. Implement and maintain an AISSP, including the preparation of policies, standards, and procedures, as appropriate.

2. Assign responsibility for the day-to-day direction of a cost-effective AISSP to an organizational level Information Systems Security Officer (ISSO), with adequate full-time equivalent staffing, equipment, and resource support. (Management has primary responsibility for the overall direction of the AISSP.)

3. Assign responsibility for the security of each AIS, AIS facility, or Information Technology Utility (ITU) to the management official most knowledgeable about the program which the AIS, AIS facility, or ITU supports, and ensure adequate training for the official.

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

5. Assign security level designations to all data files, application systems, AISs, AIS facilities, and ITUs.

6. Develop and maintain an AIS security profile.

---

[1] DHHS IRM Circular on Automated Information Systems Security Program

Security Plans

7. Identify sensitive systems, and develop and implement Computer Systems Security Plans.

Applications Security

8. Establish a control process to ensure that appropriate administrative, physical, and technical safeguards are incorporated into all new AIS applications and significant modifications. Such controls for sensitive applications must include policies and responsibilities for at least the following cases:

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

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

9. Establish a program for conducting periodic reviews and evaluations and for certifying the adequacy of the security safeguards of each AIS 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.

Personnel Security

11. Implement personnel security policies covering all individuals participating in AIS design, operation, and maintenance, or having access to data from such systems.

Information Technology Installations

12. Assign responsibility for the conduct of periodic risk analyses for each AIS facility. Such periods shall not exceed 5 years.

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

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

Security Awareness and Training

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

Reporting

16. Include A-130 security weaknesses in the annual A-123 report to the President.

17. Provide AISSP reports, as required.

18. Develop and implement a security breach reporting system.

The following table (on page I-6) provides an overview of the AISSP's basic security functions and sources of authority. This *Handbook* contains the detailed policy and guidance to satisfy these basic requirements, which, in turn, will also satisfy the security aspects of the 55 control requirements listed in the appendices.

The sources of authority listed in the following table are:

Table	Explanation
Act 1987:	The Computer Security Act of 1987, Public Law 100-235, January 8, 1988
A-130:	OMB Circular No. A-130, Appendix III, Security of Federal Automated Systems, December 12, 1985
A-123:	OMB Circular No. A-123 Revised, Internal Control Systems, August 4, 1986
A-127:	OMB Circular No. A-127, Financial Management Systems, December 19, 1984
FPM:	Federal Personnel Manual, Chapter 731, Personnel Suitability, September 29, 1988; and DHHS Instruction 731-1, Personnel Security/Suitability Policy and Technical Guidance, August 4, 1988
FIRMR:	Federal Information Resources Management Regulations (FIRMR), Part 201-7, Security of Information Resource Systems, December 1984

PA/FOIA: Privacy Act of 1974, Public Law 93-579, December 31, 1974, as amended; Freedom of Information Act, Public Law 90-23

NIST Pubs: NIST Publications, including Federal Information Processing Standards Publications (FIPS PUBS):

FIPS PUB 31, Guidelines for Automatic Data Processing Physical Security and Risk Management, June 1984

FIPS PUB 65, Guideline for Automatic Data Processing Risk Analysis, August 1, 1979

FIPS PUB 73, Guidelines for Security of Computer Applications, June 30, 1980

FIPS PUB 87, Guidelines for ADP Contingency Planning, March 27, 1981

FIPS PUB 102, Guideline for Computer Security Certification and Accreditation, September 27, 1983

NIST Special Publication 500-72, Computer Security Training Guidelines, November 1989

EXHIBIT I-A: Automated Information Systems Security Program

Basic Security Functions	Act * 1987	A-130	A-123 A-127	FPM	FIRMR	PA/ FOIA	NIST Pubs
Policy							
Implement and maintain AISSP; assign responsibilities.		X			X	X	
Security Plans							
Identify sensitive systems; implement security plans.	X				X		
Applications Security							
Certify applications systems; recertify every 3 years.		X	X		X		73, 102
Develop and maintain contingency plans.		X			X		87
Installation Security							
Conduct risk analysis every 5 years.		X	X		X		31, 65
Prepare acquisition specifications		X			X		
Maintain disaster recovery plans.		X					87
Personnel Security							
Designate sensitive 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				

* The Computer Security Act of 1987 is implemented through OMB Bulletins (OMB Bulletin No. 90-08 for 1990) and other regulatory material.

D. RESPONSIBILITIES

1. Secretary of the Department of Health and Human Services

The Secretary is responsible for the implementation and administration of an automated information systems security program within the department.

2. Assistant Secretary for Management and Budget (ASMB)

The ASMB, as the Designated Senior IRM Official, is responsible for:

a. *Overseeing the Department's AIS security program and approving associated policy.*[2]

b. Ensuring an appropriate level of protection for all Departmental 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, AISs, AIS facilities, and ITUs. This includes both physical and electronic security requirements.

3. Deputy Assistant Secretary for Information Resources Management (DAS/IRM)

The DAS/IRM is responsible for:

a. developing security policy for the Department.

b. promoting and coordinating the Department-wide AIS security program activities.

c. monitoring OPDIV AIS security program activities by:

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

2. Reviewing progress reported in the OPDIV long-range IRM plans and the annual IRM review program reports;

[2] ibid.

3. Ensuring OPDIV AIS Security Officers approve Agency Procurement Requests submitted to the Office of Information Resources Management for approval; and,

4. Evaluating safeguards used to protect major information systems.

d. as part of the on-site IRM reviews of the OPDIVs, ensuring that the OPDIVS are in conformance with DHHS AIS security policies.

e. appointing the Senior Information Systems Security Officer for the Department to assist in coordinating and evaluating the AIS security program.[3]

f. Defining and establishing the basic control requirements applicable to the four security levels of data sensitivity and the four security levels of operational criticality.

g. Establishing security program requirements for Operating Divisions (OPDIVs), Staff Divisions (STAFFDIVs), and Regional Offices (ROs).

h. Coordinating, in conjunction with the STAFFDIV heads, the AISSP for the Office of the Secretary (OS).

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

j. Providing the resources necessary to administer the Department's AISSP.

k. Performing official AISSP liaison activities with non-DHHS Government organizations and private organizations or committees, as required.

l. Coordinating the Department's AISSP with the Department's Internal Controls Program to preclude fraud, waste, and abuse with regard to the Department's information resources, and the duplication of effort across these programs.

[3] ibid.

4. Heads of Operating Divisions (OPDIVs) and Regional Directors (RDs)

OPDIV heads and RDs are responsible for:

a. *developing and implementing OPDIV security procedures, standards, and guidance consistent with Departmental and Federal requirements.*

b. *including security considerations in applications systems development, implementation, and operation and maintenance activities.*

c. *developing, implementing, and maintaining Computer Systems Security Plans for sensitive systems.*

d. *providing an objective, independent review and approval process for both Computer System Security Plans and Agency Procurement Requests to validate the adequacy of the proposed security safeguards.*

e. *establishing and administering a security awareness and training program.*

f. *establishing and administering an AIS personnel suitability/screening program.*

g. *establishing and maintaining a program for computer security certification and accreditation.*

h. *integrating the AIS security program with the internal control requirements of OMB Circular A-123.*

i. *appointing an OPDIV Senior Information Systems Security Officer to assist in the coordination of the AIS security program and participate in Department- wide security initiatives and activities.*[4]

j. Ensuring that additional OPDIV and RO security policies are developed and implemented as required for data, personnel, AISs, AIS facilities, and ITUs.

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

[4] ibid.

l. Ensuring that security level designations are assigned for AIS facilities and ITUs under their control.

m. Ensuring that appropriate risk management programs are developed, implemented, and maintained for all data, AISs, and AIS facilities under their jurisdiction. (Refer to Federal Information Processing Standards [FIPS] Publications [PUBS] 31 and 65 for additional guidance.)

n. Ensuring that appropriate contingency plans are developed, tested, and maintained within their organizations.

o. Ensuring that all application systems and automated data files within their jurisdictions are identified and that an Application System Manager is appointed for each application system and a Data File Manager is appointed for each data file.

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

q. Ensuring that a computer virus plan of action has been developed, including the selection and training of a computer virus specialist.

5. Deputy Assistant Secretary for Finance (DAS/F)

The DAS/F is responsible for coordinating the Department's Internal Controls Program with the AISSP to ensure comprehensiveness, and for establishing uniform sensitivity/criticality security level designations for the financial management systems according to the guidelines of OMB Circular A-127.

6. Deputy Assistant Secretary for Administrative and Management Services (DAS/AMS)

The DAS/AMS is responsible for:

a. Ensuring that the information resources security policies are covered in the data processing and project management training courses.

b. Ensuring that Contracting Officers enforce the sensitivity/criticality requirements designated in contracts.

c. Developing guidelines for information resources property (real and personal) management.

d. Establishing uniform AIS facility security policies.

7. Assistant Secretary for Personnel Administration (ASPER)

The ASPER is responsible for:

a. Developing personnel security guidelines, processing personnel clearance forms for each designated individual, and transferring personnel security information to other agencies. (See *DHHS Instruction 731-1, Personnel Manual.)*

b. Developing DHHS' policy for the safeguarding of documents containing classified information (i.e., *Manual for Controlling Documents Containing Classified Information)* and for monitoring implementation of these policies.

c. Initiating personnel investigations conducted by the Office of Personnel Management (OPM).

d. Providing advice and technical assistance on adult learning and instructional technology to the designers/ developers of the AIS Security Training Course and related training.

8. Heads of Staff Divisions (STAFFDIVs)

STAFFDIV heads are responsible for:

a. Ensuring that managers within their organizations are kept apprised of security requirements.

b. Administering and managing the Department's AISSP in their organizations, including establishing security level designations, as necessary, for AISs, AIS facilities, and ITUs under their control.

c. Ensuring that additional STAFFDIV security policies are developed and implemented as required for data, personnel, AISs, AIS facilities, and ITUs.

d. Ensuring that all application systems and automated data files within their jurisdictions are identified and that an Application System

Manager is appointed for each application system and a Data File Manager is appointed for each data file.

9. AIS Facility Managers and ITU Managers

AIS Facility Managers share the responsibility for:

a. Ensuring the security of the data and application systems which are stored or processed in their facilities.

b. Ensuring the basic security services for their AIS facilities, e.g., access, removal of resources, temperature control, fire protection, and electrical power.

ITU Managers share the responsibility for:

a. Ensuring the security of the data and application systems which are stored or processed in their ITUs.

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

Both AIS Facility Managers and ITU Managers are responsible for:

a. Determining the level of secure service their facilities/ ITUs are to provide, and assigning security level designations to their facilities/ITUs based on the sensitivity of the AISs and data files they need to process. (See Chapter VIII: AIS Facilities.)

b. Specifying, implementing, and reviewing procedures used to protect the integrity of their facilities/ITUs and operating systems. This involves the performance of risk analyses and the determination of minimum safety requirements and safeguards. The minimum safety requirements and safeguards for all AIS facilities are outlined in Chapter III, Exhibit III-A: Matrix of Minimum Security Safeguards.

c. Ensuring that their facilities fully comply with the physical security requirements as defined in Part 7 of the *DHHS General Administration Manual.*

d. Ensuring that the security needs of their facilities/ITUs will be and are being identified, breaches monitored, and corrective actions taken.

e. Ensuring that all AIS Managers and users of their facilities/ITUs are aware of the level of secure service offered (i.e., security designation). This includes all safeguards the facilities/ITUs offer.

f. Conducting risk analyses of their facilities/ITUs to determine cost-effective and essential security safeguards. (See Chapter V: Risk Management.)

g. Developing and maintaining contingency plans, to include designated personnel to be responsible for effecting backup operations in the event of major disruptions. (See Chapter VI: Contingency Planning.)

h. Determining the security level designations for critical and sensitive personnel positions. (See Chapter VII: Personnel Security/Suitability and Training.)

i. Working with the Project Officer, Contracting Officers, and organization ISSO to ensure that Requests for Proposals (RFPs) pertaining to their facilities/ITUs comply with the Departmental AISSP, and participating in the technical review conducted by the Project Officer of successful proposals received in response to RFPs. (See Chapter XII: Acquisitions and Contracts.)

j. Providing security for the data and application systems which are stored or processed in their facilities/ITUs.

k. Ensuring that employees under their jurisdiction receive appropriate security training.

10. Automated Information System (AIS) Managers and Application System Managers

AIS Managers are responsible for:

a. Ensuring the security of the data within their AISs, including the determination of the sensitivity/criticality security level designations for their AISs and associated data files.

b. Ensuring that appropriate security safeguards exist to adequately protect their AISs (and data files for which they are responsible) commensurate with the security level designations assigned (e.g., secure storage facilities, duplicate backup copies, alternative "contingency processing plans").

c. Notifying the organization ISSO and users of the levels of security required by their data and data processing capabilities.

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

e. Ensuring that their AISs (and data files for which they are responsible) are only run at AIS facilities and ITUs with security level designations equal to or higher than the designations of their AISs.

f. Conducting risk analyses of their AISs to determine cost-effective and essential security safeguards. (See Chapter V: Risk Management.)

g. Ensuring that data critical to the performance of their organizations have backup copies maintained, safeguarded, and ready for use in the event of a disaster. (See Chapter VI: Contingency Planning.)

h. Determining the security level designations for critical and sensitive personnel positions. (See Chapter VII: Personnel Security/Suitability and Training.)

Application System Managers are responsible for:

a. Designating the security levels of their application systems and establishing and communicating the security safeguards required for protecting their application systems, the PCs/WPs which run their application systems, and the data processed by their application systems. (See Chapter X: Personal Computers and Word Processors.)

b. Notifying the organization ISSO and users of the level of security required by their application systems.

c. Certifying that the security requirements of their application systems are being met or will be met.

d. Ensuring that their application systems are only run at AIS facilities and ITUs that are certified at a level of security equal to or higher than the security level designated for their application systems.

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

f. Conducting risk analyses of their sensitive application systems.

Both AIS Managers and Application System Managers are responsible for:

a. Documenting the rationale for those security requirements or recommendations cited in Risk Assessments/Computer System Security Plans which have not or cannot be implemented.

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

c. Working with the Project Officer, Contracting Officers, and organization ISSO to ensure that Requests for Proposals (RFPs) pertaining to their AISs/application systems comply with the Departmental AISSP, and participating in the technical review conducted by the Project Officer of successful proposals received in response to RFPs. (See Chapter XII: Acquisitions and Contracts.)

11. Data File Managers

Data File Managers are responsible for:

a. Designating the sensitivity security levels of their data files and establishing and communicating the security safeguards required for protecting them.

b. Notifying the organization ISSO and users of the level of security required by their data files.

c. Certifying that the security requirements of their data files are being met or will be met.

d. Documenting the rationale for those security requirements or recommendations cited in Risk Assessments/Computer System Security Plans which have not or cannot be implemented.

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

f. Ensuring that their data files are only run at AIS facilities and ITUs that are certified at a level of security equal to or higher than the security level designated to their data files.

12. OPDIV Senior and STAFFDIV/RO Information Systems Security Officers (ISSOs)

OPDIV Senior and STAFFDIV/RO ISSOs are responsible for:

a. Directing, coordinating, and evaluating the AISSP of their organizations.

b. Maintaining an inventory of all data files, application systems, AISs, AIS facilities, and ITUs within their organizations that have been designated with a security level of 4, 3, or 2 (Level 1 data files, AISs, etc. are optional).

13. Organization Information Systems Security Officer (ISSO) or OPDIV Senior ISSO

The ISSO in each DHHS organization, or the OPDIV Senior ISSO in an OPDIV without sublevel agencies, is responsible for:

a. Evaluating and providing information about the AISSP to the organization's management and for communicating Departmental AISSP requirements and concerns to the organization.

b. Providing advice and assistance to AIS Managers, ITU Managers, AIS Facility Managers, and other organizational personnel concerning the security of sensitive data and the security of critical data processing capabilities.

c. Reporting information resources security breaches, in accordance with the security breach reporting procedures developed and implemented by the OPDIV/STAFFDIV/RO.

d. Coordinating information resources security training activities for ITU Managers, AIS Managers, AIS Facility Managers, and AIS users.

e. Coordinating the risk management programs of their organizations with the OPDIV/RO Internal Control Officers to ensure that all risk management programs are well integrated. (See Chapter V: Risk Management.)

f. Maintaining the documentation used to establish the security level designations of all data files, application systems, AISs, AIS facilities, and ITUs within their organizations.

g. Developing, directing, and implementing risk management programs and monitoring all phases of these programs to ensure that they are conducted properly and effectively.

h. Assisting AIS Facility Managers and ITU Managers in developing policy and plans to ensure that contingency plans are either in place for AIS facilities and ITUs and/or are under active development. (See Chapter VI: Contingency Planning.)

i. Coordinating the organization's compliance with the AIS 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 PC/WP hardware and data from improper use or abuse. (See Chapter X: Personal Computers and Word Processors.)

k. Assisting Project Officers and appropriate Application System Managers/AIS Managers/AIS Facility Managers/ITU Managers in carrying out the provisions of the AISSP policy for solicitations and contracts. The organization ISSO also confirms, with his/her signature, that the successful proposals received in response to an RFP and certified by the Project Officer do indeed comply with the requirements of the Departmental AISSP. (See Chapter XII: Acquisitions and Contracts.)

14. Servicing Personnel Security Officer (SPSO)

The SPSO is responsible for processing appropriate completed personnel clearance forms for each designated individual through ASPER. (See *DHHS Instruction 731-1, Personnel Manual.)* The SPSO is also responsible for maintaining a list of encumbered positions, with a corresponding list of clearances and the date on which each clearance was granted.

15. Privacy Act Officers/Coordinators (PAO/Cs)

PAO/Cs are responsible for notifying their ISSOs of developments, deletions, or changes to automated systems of records under the Privacy Act.

16. Contracting Officers

Contracting Officers are responsible for:

a. Ensuring that all pertinent AIS security requirements specified in this *Handbook* are sufficiently detailed in each solicitation issued and contract awarded.

b. Ensuring the contractor's compliance with these security requirements.

c. Ensuring that the pre-certification statements of AIS security requirements for successful proposals are signed by both the Project Officer and organization ISSO and submitted with the proposals.

d. Including a statement in the Request for Proposal (RFP) requiring offerors to present a detailed outline of their present or proposed AIS security program in their proposals.

e. Including a statement in the RFP that offerors are required to comply with the Statement of Work (SOW) and with the requirements of the Departmental AISSP.

f. Furnishing copies of this *Handbook* when requested by offerors who respond to the RFP.

g. Forwarding any forms to the organization ISSO which the winning contractor must submit to verify or obtain personnel security clearances for his/her staff.

h. Ensuring that the technical evaluation reports developed on successful proposals by the Project Officer and his/her peers either detail any AIS security deficiencies or confirm that the contractors comply with the requirements.

17. Records Management Officers

Records Management Officers are responsible for providing consultation to Data File Managers to ensure that records retention schedules are adopted in accordance with DHHS guidance and that records disposal procedures are undertaken in accordance with the sensitivity of the data.

18. Supervisors

Supervisors are responsible for:

a. Ensuring that their employees are aware of and observe all of the security requirements of the data, AISs, AIS facilities, ITUs, and office automation equipment they use.

b. Monitoring employee activities to ensure strict compliance with all legal requirements concerning the use of proprietary software, e. g. respecting copyrights and obtaining site licenses.

c. Ensuring that only authorized software runs on government PCs and other government hardware.

19. 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 systems and data files.

c. Assisting Application System/Data File Managers in determining the required security level designations for application systems/data files.

d. Running application systems/data files only at AIS facilities and ITUs that are certified at a level of security equal to or higher than the security level designated for their application systems/data files.

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

20. Employees

Each employee is responsible for assisting in the protection of the Department'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 Department's computers and must comply with all copyright requirements.

E. CHAPTER SUMMARIES

Chapter II: Security Level Designations

This chapter explains the four data sensitivity security level designations and the four operational criticality security level designations. It describes the types of data covered by each sensitivity level and the types of data processing capabilities covered by each criticality level. AIS Managers should use the guidance provided in this chapter to determine the appropriate security levels required to protect the data and processing capabilities of their AISs.

Chapter III: Security Level Requirements

This chapter outlines the minimum security requirements of the four security level designations explained in Chapter II. The requirements apply to all AISs, AIS facilities, and ITUs under the direct or indirect jurisdiction of DHHS. This chapter also provides a list of the 40 security safeguards used within the AISSP and guidance for identifying the appropriate safeguards for every kind of AIS, AIS facility, and ITU within DHHS.

Chapter IV: AISSP Administration at the OPDIV/STAFFDIV/RO Level

This chapter outlines the responsibilities of all DHHS organizations in administering the AISSP. It explains the coordination responsibilities of the ISSO in each organization. It summarizes the responsibilities of management in coordinating the AISSP with other security programs and information resource management activities within DHHS. It outlines the AISSP reporting requirements and planning activities for the organization.

Chapter V: Risk Management

This chapter describes the basic elements of risk management at the organization level. All DHHS organizations are responsible for developing, implementing, and maintaining risk management programs to protect their data, AISs, AIS facilities, and ITUs. This chapter covers the responsibilities of management relating to risk

management and outlines the processes for risk management analysis and implementation.

Chapter VI: Contingency Planning

This chapter outlines the contingency planning process within the AISSP. The information in this chapter applies to all DHHS organizations which use automated data files and AIS facilities/ITUs. A contingency plan details how an organization would continue its mission and provide continuity of data processing in the case of a total power outage expected to last for an extended period of time. The chapter covers the contingency planning process for large AIS facilities/ITUs and office automation and personal computer AIS facilities/ITUs. The responsibilities of management and users in the contingency planning process are also addressed.

Chapter VII: Personnel Security/Suitability and Training

This chapter describes the Department's AIS Personnel Security Program. It provides guidance for determining the personnel security level designations for all positions with access to the Department's AIS resources. It outlines the requirements for background investigations of employees in sensitive positions. It describes how to deal with adverse security reports, and it presents the requirements for AIS security training. The information in this chapter applies to all DHHS personnel and all contractor personnel who have access to or participate in the design, operation, or maintenance of the Department's automated information systems.

Chapter VIII: AIS Facilities

This chapter presents the Departmental policies and guidelines for protecting the security of AIS facilities and operating systems. It outlines the security requirements and procedural safeguards for protecting the operating systems of AIS facilities, and it covers the following security requirements for protecting the physical security of AIS facilities: access control, protection of sensitive materials, AIS facility construction, and fire safety.

Chapter IX: Application Systems and Data Security

This chapter presents the AISSP policy for determining and documenting the sensitivity of automated data files and the operational criticality of application systems. The information presented in this chapter correlates closely with the information presented in Chapters II and III, concerning the security requirements and minimum security safeguards required to protect the Department's AISs, AIS facilities, and ITUs.

Chapter X: Personal Computers and Word Processors

This chapter presents the AISSP policy for protecting personal computers and word processors, and their application systems and data, from damage, destruction, or misuse. The chapter covers the general requirements for protecting the application systems and hardware of personal computers and word processors and the specific requirements for protecting sensitive data when processed by personal computers and word processors.

Chapter XI: Data Communications

This chapter presents the Departmental policy for protecting data and data communications equipment and software that transmit data by electrical, electro-mechanical, or wave energies. The policy applies to all DHHS organizations which use data communications equipment and to contractors who provide any type of ADP data communication service, software, or equipment.

Chapter XII: Acquisitions and Contracts

This chapter presents the AISSP policy for establishing appropriate security requirements for all contracts which involve the development of an AIS or the use of Departmental AIS resources. All Departmental personnel who award Government monies for AIS services must adhere to the policy guidelines presented in this chapter, whether the services are procured by DHHS or the General Services Administration (GSA). All contractors who are involved in developing automated information systems for use by DHHS, or in providing any other type of service for the Department in which AIS resources are used, must agree to comply with the requirements of the Departmental AISSP and this chapter.

Appendices

Includes five appendices: the general references used in developing the *AISSP Handbook*; a listing of 55 control requirements which constitute the core of the Departmental AISSP; a cross-reference table showing the principal control directives from which each of the 55 controls was established; definitions of common terms used in the *AISSP Handbook;* and definitions of all acronyms used in the *AISSP Handbook.*

CHAPTER II. SECURITY LEVEL DESIGNATIONS

A. OVERVIEW

The security efforts of the Automated Information Systems Security Program (AISSP) are based on the sensitivity of data contained in Automated Information Systems (AISs) and the operational criticality of the data processing capabilities of AISs. Sensitivity/criticality security level designations are used to define the requirements of these security efforts. AIS Managers are responsible for identifying the appropriate sensitivity/criticality security level designations for their AISs.

The purpose of this chapter is to provide guidance for the determination of security levels. AIS Managers should use the guidance in this chapter and, as appropriate, supplemental guidance issued by their organizations, to determine the required security for their AISs. The actual security requirements for each security level designation are detailed in Chapter III: Security Level Requirements.

B. INTRODUCTION TO SECURITY LEVELS

The security level designations within the AISSP 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 four security level designations for data sensitivity and four security level designations for operational criticality. Obviously, some data within an AIS are more sensitive than other data, i.e., an AIS might be so compartmentalized that one level of security is appropriate for one set of data and a different level for another set. This also applies to the criticality security levels associated with data processing. An AIS might be so compartmentalized that one level of security is appropriate for one process and a different level for another process. In most instances, however, it is not possible to identify independent processes within an AIS. In all instances, the security level designation of an AIS as a whole should be equal to or higher than the highest security level designation of any data it processes. This will help insure that the security requirements for data and AISs appropriately address the classical

automated information security "CIA" issues, i.e., the level of data and AIS Confidentiality, Integrity, and Availability safeguarding desired.

AIS Managers must ensure that their data files and the processing capabilities of their AISs are only accessed by authorized users who fully utilize the required security level safeguards. The managers of compartmentalized AISs should take special care to specify the appropriate level of security required when negotiating with an AIS facility, Information Technology Utility (ITU), or contractor for services.

To summarize, the Department's security level designations determine the minimum security safeguards required to protect sensitive data files and to ensure the operational continuity of critical data processing capabilities.

C. SENSITIVITY SECURITY LEVELS FOR DATA FILES

Sensitivity security level designations are assigned to data files based on the type of data in the files and the requirements of specific laws governing the protection or disclosure of information, e.g., the Privacy Act. A Level 1 designation is used for data files with the least sensitive data, and a Level 4 designation is used for files with the most sensitive data.

1. Level 1: Low Sensitivity

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

   a. Data files which 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. Data files which require safeguarding by the Privacy Act, but 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 to have no adverse impact on the individual.

2. Level 2: Moderate Sensitivity

   This category identifies data that have some importance to the Agency and which must be protected against such acts as malicious destruction. However,

since much of these data are 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 need to be restricted only to a limited degree. These 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 DHHS programs to the public. These data need protection commensurate with the value of the information to the organization. Loss of this kind of data should not be potentially embarrassing or detrimental to an individual or business.

c. Data files that require safeguarding by the Privacy Act but which contain information that could cause only nonspecific embarrassment to an individual if properly disclosed, or which could identify individuals by statistical configuration.

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

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

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

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

d. Data files that require safeguarding by the Privacy Act but 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.

4. Level 4: High Sensitivity and National Security Interest

This category identifies all data files which contain national security classified information and all data files which contain other sensitive, but unclassified information, the loss of which could adversely affect national security interests. (DHHS) does not have the authority to originate classified material, and Operating Divisions (OPDIVs)/Staff Divisions (STAFFDIVs)/Regional Offices (ROs) should not automate, create, or store classified information without prior Departmental approval.)

D. CRITICALITY SECURITY LEVELS FOR APPLICATION SYSTEMS

Criticality security levels are assigned to AISs based upon the relative importance of their processing capabilities to the organizations they support. A Level 1 designation is used for an AIS with the lowest criticality of data processing relative to the organization it supports; and a Level 4 designation is used for an AIS with the highest criticality.

1. Level 1: Low Criticality

This category identifies AISs with data processing capabilities that require minimal protection. These include AISs whose alteration or failure would have a minimal impact on their organizations and/or which could be easily replaced with a minimum of staff time or expense. This category also includes AISs which generate, store, process, transfer, or communicate data which are considered to have low or no sensitivity.

2. Level 2: Moderate Criticality

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

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

b. AISs which generate, store, process, transfer, or communicate data which are considered to have moderate sensitivity (Level 2).

3. Level 3: High Criticality

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

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

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

c. AISs which generate, store, process, transfer, or communicate data which are considered to have high sensitivity (Level 3).

4. Level 4: High Criticality and National Security Interest

This category identifies all AISs with data processing capabilities that are considered critical to the well-being of the nation. For example:

a. AISs which generate, store, process, transfer, or communicate national security classified data.

b. AISs which handle other sensitive, but unclassified information, the loss of which could adversely affect national security interests.

National Security Decision Directive No. 145 (NSDD-145), "National Policy on Telecommunications and Automated Systems Security," requires that these AISs "shall be protected in proportion to the threat of (compromise or) exploitation and the associated potential damage to the national security."

CHAPTER III. SECURITY LEVEL REQUIREMENTS

A. OVERVIEW

This chapter outlines the minimum security requirements for the four security level designations explained in Chapter II of this *Handbook*. The security requirements apply to all Automated Information Systems (AISs), AIS facilities, and Information Technology Utilities (ITUs) under the direct or indirect jurisdiction of DHHS, including those that are operated by Government Agencies other than DHHS and by contractors functioning as agents of DHHS.

The higher the security level designation of an AIS, AIS facility, or ITU, the more stringent its security requirements. AISs, AIS facilities, and ITUs 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 AISs, AIS facilities, or ITUs 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 batch and on-line systems. AIS Managers, AIS Facility Managers, and ITU Managers must continually evaluate their systems to determine if they can be circumvented and must test their security safeguards to ensure that they are functioning as intended. Reviews are required at least once every 3 years. Additional reviews are required if the safeguard requirements outlined in this chapter change or if an AIS, AIS facility, or ITU undergoes a significant modification. A waiver must be requested prior to certification if an AIS, AIS facility, or ITU is not in compliance and cannot be brought into compliance in a relatively short period of time, or if an Operating Division/Staff Division (OPDIV/STAFFDIV) head or Regional Director (RD) disagrees with a particular safeguard requirement.

B. RESPONSIBILITIES

1. Assistant Secretary for Management and Budget (ASMB)

   The ASMB is responsible for issuing the security program requirements and guidelines for data, AISs, AIS facilities, and ITUs. This includes both physical and electronic security requirements.

2. Heads of Operating and Staff Divisions (OPDIV/STAFFDIVs) and Regional Directors (RDs)

   OPDIV/STAFFDIV heads and RDs are responsible for:

   a. Ensuring that security level designations are assigned for AIS facilities and ITUs under their control.

   b. Ensuring that additional OPDIV/STAFFDIV/Regional Office (RO) security policies are developed and implemented as required for data, personnel, AISs, AIS facilities, and ITUs.

3. Automated Information System (AIS) Managers

   AIS Managers are ultimately responsible for the physical and electronic security of their data and the data processing capabilities of their AISs. This includes:

   a. Determining the sensitivity/criticality security level designations for their AISs and associated data files.

   b. Notifying the organization Information Systems Security Officer (ISSO) and users of the levels of security required by their data and data processing capabilities.

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

   d. Ensuring that their AISs (and data files for which they are responsible) are only run at AIS facilities and ITUs with security level designations equal to or higher than the designations of their AISs.

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

4. Information Technology Utility (ITU) and AIS Facility Managers

   ITU and AIS Facility Managers are responsible for the security of the data and AIS processing capabilities which are stored or processed in their facilities or ITUs. This includes:

   a. Determining the level of secure service their facilities/ITUs are to provide, and assigning security level designations to their facilities/

ITUs based on the sensitivity of the AISs and data files they need to process.

b. Specifying, implementing, and reviewing procedures used to protect the integrity of their facilities/ITUs and operating systems. This involves the performance of risk analyses and the determination of minimum safety requirements and safeguards.

c. Ensuring that the security needs of their facilities/ITUs will be and are being identified, breaches monitored, and corrective actions taken.

d. Ensuring that all AIS Managers and users of their facilities/ITUs are aware of the level of secure service offered (i.e., security designation). This includes all safeguards the facilities/ITUs offer and any waivers received.

5. OPDIV Senior and STAFFDIV/RO Information Systems Security Officers (ISSOs)

OPDIV Senior ISSOs and STAFFDIV/RO ISSOs are responsible for maintaining an inventory of the security level designations for all data files, application systems, AISs, AIS facilities, and ITUs within their organizations.

6. Supervisors

Supervisors are responsible for ensuring that their employees are aware of and observe all of the security requirements of the data, AISs, AIS facilities, ITUs, and office automation equipment they use.

C. SECURITY LEVEL REQUIREMENTS

1. Level 1 Requirements

The controls required to adequately safeguard a Level 1 AIS, AIS facility, or ITU are those which would normally be considered good management practice. These include, but are not limited to:

a. An employee AIS security awareness and training program.
b. The assignment of sensitivity designations to every employee position.
c. Physical access controls.
d. A complete set of AIS documentation.

2. Level 2 Requirements

The controls required to adequately safeguard a Level 2 AIS, AIS facility, or ITU include all of the requirements for a Level 1, plus the following requirements:

a. A detailed risk management program.
b. Record retention procedures.
c. A list of authorized users.
d. Security review and certification procedures.
e. Clearance (i.e., appropriate background checks) to occupy every employee position.
f. Clearance (i.e., appropriate background checks) for all contractor personnel.
g. A detailed fire/catastrophe plan.
h. A formal written contingency plan.
i. A formal risk analysis.
j. An automated audit trail.
k. Authorized access and control procedures.
l. Secure physical transportation procedures.
m. Secure telecommunications.
n. An emergency power program.

3. Level 3 Requirements

The controls required to adequately safeguard a Level 3 AIS, AIS facility, or ITU include all of the requirements for Levels 1 and 2, plus the requirement for an inventory of hardware and software.

4. Level 4 Requirements

The controls required to adequately safeguard a Level 4 AIS, AIS facility, or ITU include all of the requirements for Levels 1, 2, and 3, plus the following requirements:

a. The requirements of National Security Decision Directives, and other Federal Government directives, for data and systems that are classified.

b. The security procedures specified by the source agencies that provide the classified information or systems to DHHS.

D. MATRIX OF MINIMUM SECURITY SAFEGUARDS

A comprehensive Matrix of Minimum Security Safeguards has been established to identify the minimum security safeguards that are required to protect any type of AIS facility or ITU with any security level rating. The Matrix appears on the following pages. An X on the matrix means that a security safeguard is a requirement for an AIS facility or ITU with a certain security level 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 AIS facility or ITU, regardless of its security level designation.

EXHIBIT III-A: MATRIX OF MINIMUM SECURITY SAFEGUARDS

Explanation: This matrix is used to identify a minimum set of safeguards by sensitivity/criticality security level which should be implemented to protect AISs, AIS facilities, and/or ITUs.

Justification for non-implementation of these safeguards should be based on the results of a formal risk analysis (and cost benefit) study.

Directions: Scan the Xs and Os beneath each security level designation. An X means that the security safeguard listed to the left is a requirement. An O means that the security safeguard is optional.

	SECURITY LEVEL			
	High Sensitivity/ Criticality National Security (Level 4)	High Sensitivity/ Criticality (Level 3)	Moderate Sensitivity/ Criticality (Level 2)	Low Sensitivity/ Criticality (Level 1)
1. Ensure that a complete and current set of documentation exists for all operating systems.	X	X	X	X
2. Require use of current passwords and log-on codes to protect sensitive automated information systems data from unauthorized access.	X	X	X	O
3. Establish procedures to register and protect secrecy of passwords and log-on codes, including the use of a nonprint, nondisplay feature.	X	X	X	O
4. Limit the number of unsuccessful attempts to access an automated information system or a data base.	X	X	X	O
5. Develop means whereby the user's authorization can be determined. (This may include answerback capability.)	X	X	X	O
6. Establish an automated audit trail capability to record user activity.	X	X	X	O
7. Implement methods, which may include the establishment of encryption, to secure data being transferred between two points.	X	X	O	O
8. Ensure that the operating system contains controls to prevent unauthorized access to the executive or control software system.	X	X	X	O
9. Ensure that the operating system contains controls that separate user and master modes of operations.	X	X	X	O
10. Record occurrences of nonroutine user/operator activity (such as unauthorized access attempts and operator overrides) and report to the organizational ISSO.	X	X	O	O
11. Ensure that the operating system provides methods to protect operational status and subsequent restart integrity during and after shutdown.	X	X	O	O

EXHIBIT III-A: MATRIX OF MINIMUM SECURITY SAFEGUARDS

	SECURITY LEVEL			
	High Sensitivity/ Criticality National Security (Level 4)	High Sensitivity/ Criticality (Level 3)	Moderate Sensitivity/ Criticality (Level 2)	Low Sensitivity/ Criticality (Level 1)
12. Install software feature(s) that will automatically lock out the terminal if it is not used for a predetermined period of lapsed inactive time, for a specified time after normal closing time, or if a password is not entered correctly after a specified number of times.	X	X	X	O
13. Ensure that the operating system contains controls to secure the transfer of data between all configuration devices.	X	O	O	O
14. Establish controls over the handling of sensitive data, including labelling materials and controlling the availability and flow of data.	X	X	X	O
15. Require that all sensitive material be stored in a secure location when not in use.	X	X	X	O
16. Dispose of unneeded sensitive hard copy documents and erase sensitive data from storage media in a manner which will prevent unauthorized use.	X	X	X	O
17. Prepare and maintain lists of persons authorized to access facilities and automated information systems processing sensitive data.	X	X	X	O
18. Establish procedures for controlling access to facilities and automated information systems processing sensitive data.	X	X	X	X
19. Furnish locks and other protective measures on doors and windows to prevent unauthorized access to computer and support areas.	X	X	X	X
20. Install emergency (panic) hardware on "emergency exit only" doors. Ensure that emergency exits are appropriately marked.	X	X	X	X
21. Specify fire-rated walls, ceilings, and doors for construction of new computer facilities or modifications of existing facilities.	X	X	O	O
22. Install smoke/fire detection systems with alarms in the computer facility. When feasible, connect all alarms to a control alarm panel within the facility and to a manned guard station or fire station.	X	X	O	O
23. Install fire suppression equipment in the computer facility which may include area sprinkler systems with protected control valves, and/or fire extinguishers.	X	X	X	O

EXHIBIT III-A: MATRIX OF MINIMUM SECURITY SAFEGUARDS

	SECURITY LEVEL			
	High Sensitivity/ Criticality National Security (Level 4)	High Sensitivity/ Criticality (Level 3)	Moderate Sensitivity/ Criticality (Level 2)	Low Sensitivity/ Criticality (Level 1)
24. Provide emergency power shutdown controls to shutdown AIS equipment and air conditioning systems in the event of fire or other emergencies. Include protective covers for emergency controls to prevent accidental activation.	X	X	X	O
25. Provide waterproof covers to protect computers and other electronic equipment from water damage.	X	X	O	O
26. 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	X	O
27. Secure communication lines.	X	X	X	O
28. Conduct Tempest testing of operating system.	X	O	O	O
29. Ensure that all requirements of NSDD-145 (National Security Decision Directive) are met.	X	O	O	O
30. Establish detailed risk management program.	X	X	X	O
31. Conduct formal risk analyses.	X	X	X	O
32. Establish employee security awareness and training program.	X	X	X	X
33. Maintain accurate inventory of all hardware and software.	X	X	X	X
34. Establish security review and certification program.	X	X	X	O
35. Establish contingency plan.	X	X	X	O
36. Establish emergency power program.	X	X	X	O
37. Ensure that all personnel positions have been assigned security level designations.	X	X	X	X
38. Conduct periodic security level designation reviews.	X	X	X	O
39. Ensure that all personnel, including contractors, have received appropriate clearances.	X	X	X	O
40. Maintain list of all "classified," 4C "Special Sensitive," and 3C "Critical + Sensitive," clearances granted.	X	X	O	O

CHAPTER IV. AISSP ADMINISTRATION AT THE OPDIV/STAFFDIV/RO LEVEL

A. OVERVIEW

This chapter describes the requirements for Automated Information Systems Security Program (AISSP) administration at the organization level. Each Operating Division/Staff Division (OPDIV/STAFFDIV) head and Regional Director (RD) within DHHS is responsible for meeting the requirements described in this chapter. These requirements include, but are not limited to, coordinating the activities of their organization's AISSP with the Department, reporting the status of their AISSP to the Department, establishing security breach reporting procedures, and conducting periodic security assessments.

B. ORGANIZATION INFORMATION SYSTEMS SECURITY OFFICER (ISSO)

Under the direction of their organization's management, the senior ISSO in each DHHS organization is responsible for evaluating and providing information about the AISSP of the organization to the Department and for communicating Departmental AISSP requirements and concerns to the organization. Specifically, the senior ISSO is responsible for:

1. Ensuring that security plans are developed, reviewed, implemented, and revised, as needed, for the OPDIV.

2. Providing advice and assistance to Automated Information System (AIS) Managers, Information Technology Utility (ITU) Managers, AIS Facility Managers, and other organizational personnel concerning the security of sensitive data and the security of critical data processing capabilities.

3. Reporting information resources security breaches, in accordance with the security breach reporting procedures developed and implemented by the OPDIV/STAFFDIV/Regional Office (RO).

4. Coordinating information resources security training activities for ITU Managers, AIS Managers, AIS Facility Managers, and AIS users.

C. MANAGEMENT RESPONSIBILITIES

The management of each DHHS organization is responsible for developing, implementing, maintaining, and reviewing the organization's AISSP. Management is also responsible for coordinating the organization's AISSP with other programs in the Department. This includes coordinating the organization's AISSP with other DHHS security programs and DHHS Information Resources Management (IRM) activities.

1. Coordinating the Organization's AISSP with Other Security Programs within the Department

   Various Department staff manuals and other documents established by functional departmental managers contain requirements which have an impact on an organization's AISSP. The management of each DHHS organization is responsible for coordinating the organization's AISSP with the requirements of these publications. The publications include, but are not limited to:

   a. Classified data (see the *Assistant Secretary for Personnel Administration (ASPER) Classified Document Manual).*

   b. Building security requirements (see the *DHHS General Administration Manual*, Chapter 7, Physical Security Policy).

   c. Internal controls requirements (see the *DHHS Internal Controls Manual).*

   d. Security clearance requirements for sensitive positions (see DHHS Instruction 731-1, *Personnel Manual).*

   e. Privacy and Freedom of Information Act requirements (see 45 *Code of Federal Regulations (CFR)* and *DHHS General Administration Manual,* Part 45).

   f. Management of electronic records (see the National Archives and Records Administration Guidance).

2. Coordinating the Organization's AISSP with Other IRM Activities within the Department

   The management of each DHHS organization is responsible for coordinating the organization's AISSP with the following IRM activities:

a. IRM Strategic Plan

OPDIV/STAFFDIV heads and RDs must prepare an annual update of their IRM strategic plan as described in the annual DHHS Call for Long-Range IRM Plans. All updates should recommend improvements to their AISSPs, with particular reference to the security needs of AIS facilities, ITUs, and AISs concerning data sensitivity and the criticality of data processing capabilities.

b. IRM Reviews

OPDIV/STAFFDIV heads and RDs must plan, conduct, and report IRM Reviews, as required by the Departmental IRM Review Program.

c. Information Technology Systems (ITS) Budget

OPDIV/STAFFDIV heads and RDs must prepare an annual ITS Budget as described in Part 3 of the *IRM Manual.* The budget should include the projected costs for implementing, maintaining, and improving the AISSP of their organizations as part of their short-term and long-term budget processes.

d. Automated Information Systems Inventory (AISI)

The management of each DHHS organization is responsible for including criticality and sensitivity security level designations in the AISI.

e. Internal Controls Review (ICR) Program Plans

The Department establishes ICR Program Plans each year which prioritize ICRs for the coming year. To maximize efficiency and minimize duplication of effort, the management of each DHHS organization is responsible for coordinating the Department's ICR Program Plans with the goals and objectives of the AISSP of their organization.

D. AISSP REPORTING AND OVERSIGHT

Annual AISSP reporting and DHHS oversight will be part of the integrated IRM program. The management of each DHHS organization is responsible for preparing and submitting reports on their AISSP to the Department. Reporting and oversight activities include the following:

1. DHHS IRM Call for Long-Range Plans

   The OPDIVs should discuss their internal security programs focusing on three perspectives:

   a. Sensitive system plans and their independent assessment;

   b. Computer systems security awareness and training; and

   c. Risk analysis for computer systems and installations.

   For each of the three system perspectives, the OPDIVs should provide information detailing: (1) recent progress or accomplishments over the past year; (2) current status, and (3) plans for the near-term.

2. IRM Review Program Reports

   The annual DHHS IRM Review Report was expanded in 1990 to include CSSP implementation and training status reports. Future review reports will include:

   a. A schedule of security reviews to be conducted, including reviews of Level 3 and Level 4 AISs, AIS facilities, and ITUs, at a minimum.

   b. A description of the organization's AIS security awareness and training program, including a list of available training items, such as pamphlets, videotapes, and posters.

   c. A profile of the organization's AIS facilities, personnel, and personnel security training accomplishments and needs (see Exhibit IV-A: AIS Security Resource Survey).

   d. A report of the security weaknesses reportable under the Internal Controls Program.

3. Special Reports

   These special reports are event-driven such as those required for senior-level meetings and presentations.

4. Oversight

As part of the on-site IRM reviews of the OPDIVs, OIRM will ensure that the OPDIVs are in conformance with the Computer Security Act of 1987, OMB Circular A-130, OMB Bulletins, the *AISSP Handbook*, and other requirements, as appropriate. In addition, OIRM oversight activities will include, e.g.:

a. Reviewing an annual sample of OPDIVs security plans for sensitive systems;

b. Reviewing progress reported in the OPDIV long-range IRM plans and the annual IRM review program reports;

c. Ensuring OPDIV AIS Security Officers approve Agency Procurements Requests submitted to the Office of Information Resources Management for approval; and,

d. Evaluating safeguards used to protect major information systems.

5. AISSP Security Profile

The AISSP Security Profile consists of the procedures and documentation required to support an organization's AISSP. A copy of the documents which comprise the Profile should be maintained in a single location, except when impractical, in which case the locations of the documents should be identified. The Profile should include:

a. The AIS security policies issued by the organization, including AISSP security manuals and security breach reporting procedures.

b. A copy of the Federal statutory and regulatory requirements for AIS security, including at a minimum the Computer Security Act of 1987, OMB Circular A-130, the current OMB security bulletin, and the basic NIST publications for risk management, training, and certification and accreditation.

c. A list of the organization's ISSOs, including their organizational components, work locations, and phone numbers.

d. A copy of the Computer System Security Plan (CSSPs) for the OPDIV.

e A copy of the OPDIV's Management Plan for implementing the CSSPs.

f. A copy of review comments made by any internal or external review team within the last three years.

g. A copy of the Certification/Accreditation Statement for each of the OPDIV's sensitive applications.

h. A list of designations of position sensitivity levels.

i. A list of the organization's AIS Managers, AIS Facility Managers, and ITU Managers, with their locations and phone numbers.

j. The organization's AIS inventory.

k. The organization's risk analysis reports.

l. The organization's contingency plans.

m. A copy of the report of any external reviews of the organization's sensitive applications, CSSPs, and AISSP.

E. SECURITY ASSESSMENTS

1. Purpose

Each DHHS organization is required to conduct periodic reviews and evaluations of its AISs, AIS facilities, ITUs, and AISSP for the purpose of recertifying the adequacy of the organization's security safeguards. Three types of security reviews are required:

a. A **Recertification** must be conducted at least once every 3 years for each AIS application, as required by OMB Circular A-130, Appendix III.

b. A **Risk Analysis** must be conducted at least once every 5 years for each AIS facility and ITU. The requirements for this type of security review are also outlined in OMB Circular A-130, Appendix III.

b. An **Internal Controls Review** (ICR) of the organization's AISSP must be conducted at least once every 5 years. The requirements for this type of review are outlined in OMB Circular A-123 and the *DHHS*

Internal Controls Manual. The purpose of this type of review is to guarantee the integrity of the organization's AISSP.

The management of each DHHS organization is responsible for coordinating these three assessments both within its organization and with the Department's ICR Program. This coordination is required in order to set consistent priorities, minimize duplication of effort, and ensure the total integrity of the Departmental AISSP.

CHAPTER V. RISK MANAGEMENT

A. OVERVIEW

In accordance with the requirements of the Departmental Automated Information Systems Security Program (AISSP), all DHHS organizations must develop, implement, and maintain risk management programs to ensure that appropriate safeguard measures are taken to protect all data, Automated Information Systems (AISs), AIS facilities, and Information Technology Utilities (ITUs).

The purpose of this chapter is to describe the basic elements of a successful risk management program at the organization 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 analysis followed by safeguard selection and implementation.

B. RESPONSIBILITIES

1. Heads of Operating Divisions (OPDIVs) and Regional Directors (RDs)

   OPDIV heads and RDs are responsible for ensuring that appropriate risk management programs are developed, implemented, and maintained for all data, AISs, and AIS facilities under their jurisdictions. (Refer to Federal Information Processing Standards [FIPS] Publications 31 and 65 for additional guidance.)

2. Organization Information Systems Security Officers (ISSOs)

   Organization ISSOs are responsible for:

   a. Coordinating the risk management programs of their organizations with the OPDIV/Regional Office (RO) Internal Control Officers to ensure that all risk management programs are well integrated.

   b. Developing, directing, and implementing risk management programs and monitoring all phases of these programs to ensure that they are conducted properly and effectively.

3. AIS Managers, AIS Facility Managers, ITU Managers, and Application System Managers

AIS, AIS Facility, and ITU Managers are responsible for conducting risk analyses of their AISs, AIS facilities, and ITUs to determine cost-effective and essential security safeguards. Application System Managers are responsible for conducting risk analyses of their sensitive application systems.

C. RISK MANAGEMENT PROGRAM

Each DHHS organization must develop a comprehensive risk management program. It is probably impossible to eliminate risk completely, but managers need to be aware of potential risks and vulnerabilities to their data, AISs, AIS facilities, and ITUs. 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 AIS security alternatives/safeguard options.

A risk analysis 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 analysis application package can permit responsible managers to conduct analyses more frequently, and offer a cost-beneficial approach to risk performance. A waiver must be requested if a risk analysis shows noncompliance with security requirements (see Chapter III) and compliance cannot be achieved within a relatively short period of time.

Risk management programs consist of the following processes:

Risk Analysis

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 Analysis Process

The objective of a formal risk analysis is to determine the current security status of a sensitive application system, AIS, AIS facility, or ITU. First, specific threats and vulnerabilities are discovered and analyzed. Next, potential safeguards are evaluated to select those which are most cost-effective in addressing the threats and eliminating or reducing the vulnerabilities to an acceptable level. Last, a final report is prepared which summarizes the findings and presents a set of prioritized recommendations. The final report of several risk analyses 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, AIS, AIS facility, or ITU. 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 analysis must develop a summary list of threats for every aspect of the sensitive application system, AIS, AIS facility, or ITU.

b. Vulnerability Identification

Vulnerability identification involves the determination of weaknesses or flaws present in a sensitive application system, AIS, AIS facility, or ITU which could allow a threat to affect its security. Vulnerability identification should be performed on new, existing, and recently modified sensitive application systems, AISs, AIS facilities, and ITUs.

The risk analysis must develop a summary list of vulnerabilities for each sensitive application system, AIS, AIS facility, and ITU 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 determining threats and vulnerabilities, the risk analysis must quantify the value of potential losses. The dollar is used as a common unit of measure in these assessments.

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 to the user of delayed processing. Whenever time loss is the critical unit in a case, such as a medical life support system, or the generation of income checks, the analysis should note this fact. ISSOs assist in the estimation of potential losses. The final product of this effort is a list of costs that could be incurred (both one-time costs and recurring costs).

d. Safeguard Analysis

The risk analysis next identifies possible safeguards and their related costs, after evaluating the worksheets. The analysis must ensure that the safeguards identified fulfill the minimum security safeguard requirements outlined in Chapter 3 of this *Handbook* (Exhibit III-A: Matrix of Minimum Security Safeguards).

e. Cost-Benefit Analysis

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

f. Final Report

When the risk analysis is complete, a final report is prepared, which should include the following items:

(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/ vulnerability/safeguard situation.

(4) Recommended safeguards (i.e., those safeguards which will provide the best protection considering their cost and the risks they are negating).

g. Summary Risk Assessment File

For larger organizations, a Summary Risk Assessment File, which accumulates output data from numerous risk analyses of various organizations into a single file, will provide management officials and the ISSO with knowledge about common weaknesses and strengths, permitting the development of policy covering a wide range of activity.

The OPDIV heads and RDs are responsible for ensuring the establishment of a schedule for conducting risk analyses within their respective organizations.

Managers must conduct risk analyses at a frequency commensurate with the sensitivity of their application systems or the information they process. They must also conduct analyses whenever there are major changes to a sensitive application system, AIS, AIS facility, or ITU. Managers must retain all risk analysis reports and supporting documentation for at least five years.

2. Safeguard Selection and Implementation

a. Management Decisions

This phase deals with the selection of safeguards that will reduce and/or prevent the effects of identified threats and vulnerabilities.

AIS Managers, AIS Facility Managers, ITU Managers, and the managers of sensitive application systems, with the assistance of the organization ISSO, should review the risk analysis reports and select specific security safeguards which permit the greatest reduction in exposure for the least total cost. As part of this process, managers should identify any safeguards which can protect multiple application systems, AISs, AIS facilities, and ITUs. They should also identify any actual or potential safeguards in a system which may have a negative effect on another system. (The organization ISSO can help affected managers to resolve these problems.)

In some cases, the management decisions may require the organization ISSO, through an OPDIV head or RD, to submit a request for a waiver from a security requirement, because the benefits of a security safeguard do not justify the costs. In such situations, the responsible management official assumes the risk for any waived requirements. DHHS organizations may request authorizations from the Deputy Assistant Secretary for Information Resources Management (DAS/IRM) either not to comply or to delay compliance with Federal security standards or Departmental security policy.

b. Implementation

AIS Managers, AIS Facility Managers, ITU Managers, and the managers of sensitive application systems, in coordination with the organization ISSO, should 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.

Managers should also develop a plan for monitoring the scheduled implementation of safeguards. The organization ISSO should review and approve all implementation plans for accuracy and adequacy.

Whenever the safeguards on an automated Privacy Act System of records are significantly altered as the result of a risk analysis, the organization's Privacy Act Officer/Coordinator must be notified.

D. COMPUTER VIRUSES AND RELATED THREATS

Computer viruses and related threats are becoming a serious risk management problem. OPDIVs must address these risks through a virus prevention and containment problem. NIST Special Publication 500-166, provides guidance.

1. NIST Special Publication 500-166, *Computer Viruses and Related Threats: A Management Guide*, dated August 1989, is quoted in part:

What Are Computer Viruses and Related Threats?

Computer viruses are the most widely recognized example of a class of programs written to cause some form of intentional damage to computer systems or networks. A computer virus performs two basic functions: it copies itself to other programs, thereby infecting them, and it executes the instructions the author has

included in it. Depending on the author's motives, a program infected with a virus may cause damage immediately upon its execution, or it may wait until a certain event has occurred, such as a particular date and time. The damage can vary widely, and can be so extensive as to require the complete rebuilding of all system software and data. Because viruses can spread rapidly to other programs and systems the damage can multiply geometrically.

Related threats include other forms of destructive programs such as Trojan horses and network worms. Collectively, they are sometimes referred to as malicious software. These programs are often written to masquerade as useful programs, so that users are induced into copying them and sharing them with friends and work colleagues. The malicious software phenomena is fundamentally a people problem, as it is authored and initially spread by individuals who use systems in an unauthorized manner. Thus, the threat of unauthorized use, by unauthorized and authorized users, must be addresses as a part of virus prevention.

What Are the Vulnerabilities They Exploit?

Unauthorized users and malicious software may gain access to systems through inadequate system security mechanisms, through security holes in applications or systems, and through weaknesses in computer management, such as the failure to properly use existing security mechanisms. Malicious software can be copied intentionally onto systems, or be spread when users unwittingly copy and share infected software obtained from public software repositories, such as software bulletin boards and shareware. Because malicious software often hides its destructive nature by performing or claiming to perform some useful function, user's don't generally suspect that they are copying and spreading the problem.

Steps Toward Reducing Risk

Include the damage potential of viruses, unauthorized use, and related threats in risk analysis and contingency planning. Develop a plan to deal with potential incidents.

Make computer security education a prerequisite to any computer use. Teach users how to protect their systems and detect evidence of tampering or unusual activity.

Ensure that technically oriented security and management staff are in place to deal with security incidents,

Use the security mechanisms that exist in your current software. Ensure that they are used correctly. Add to them as necessary.

A. OVERVIEW

Each DHHS organization is responsible for developing and testing a formal contingency plan for each of its major Automated Information System (AIS) facilities and Information Technology Utilities (ITUs) at Level 3 or 4. 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 documented in the organization's Automated Information Systems Security Program (AISSP).

This chapter describes the contingency planning process at the organization level. The process includes development, maintenance, testing, and implementation. The information in this chapter applies to all DHHS organizations which use automated data files and AIS facilities/ITUs, 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.

B. RESPONSIBILITIES

1. Heads of Operating Divisions (OPDIVs) and Regional Directors (RDs)

   OPDIV heads and RDs are responsible for ensuring that appropriate contingency plans are developed, tested, and maintained within their organizations.

2. Organization Information Systems Security Officer (ISSO)

   The ISSO in each DHHS organization is responsible for assisting AIS Facility Managers and ITU Managers in developing policy and plans to ensure that contingency plans are either in place for AIS facilities and ITUs and/or are under active development.

3. AIS Facility Managers and ITU Managers

AIS Facility/ITU Managers are responsible for developing and maintaining contingency plans, to include designated personnel to be responsible for effecting backup operations in the event of major disruptions.

4. AIS Managers

AIS Managers are responsible for ensuring that backup copies of data critical to the performance of their organizations are maintained, safeguarded, and ready for use in the event of a disaster.

5. Users

Users are responsible for assisting in the development of contingency plans. In particular, this responsibility involves determining which parts of automated processes can revert to manual processing and which parts need priority automated processing.

C. INTRODUCTION TO THE CONTINGENCY PLANNING PROCESS

Every AIS facility and ITU (including Wide Area Networks and Local Area Networks) which processes applications that are critical to the performance of the organizational mission it supports must have a contingency plan. However, there are major differences in the level of detail required in a contingency plan for a large AIS facility/ITU based on mainframes or minicomputers and for an AIS facility/ITU based on office automation and personal computer equipment. Therefore, after a brief discussion of the contingency planning steps both types of AIS facilities/ITUs have in common, this chapter treats the contingency planning processes separately, with the major emphasis on contingency planning for large AIS facilities/ITUs.

Each DHHS 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. For example, an AIS Facility Manager may provide an alternate power source for the computer room, but that will not help end users who need access to a mainframe at their workstations in critical locations--such as hospital workstations needing patient medical data--when power goes off there.

The following are some of the steps which organizations with completed contingency plans have used in their development process and which are common to both large

AIS facilities/ITUs and AIS facilities/ITUs based on office automation and personal computer equipment. (See Chapter X for a full discussion of personal computers and office automation equipment.)

1. Identify critical applications.

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

3. Backup critical applications, data, operating software, and databases regularly.

4. Explore alternate AIS processing sites within or outside the organization.

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

6. Develop alternate site operating procedures.

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

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

9. Continue to test regularly.

10. Update the contingency plan based on test results.

D. CONTINGENCY PLANNING PROCESS FOR LARGE AIS FACILITIES/ITUs

1. Elements of the Plan

The following elements should be included in the contingency plans for large AIS facilities/ITUs.

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 AIS facility/ITU. Furthermore, there should be reasonable assurance that the alternate site will be available in the event of a disaster and 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 to have each site serve as a backup. This strategy requires that inputs and outputs can be diverted from a disabled site, and that excess processing capacity is available to handle increased workloads on a temporary basis.

If alternative sites do not exist within the organization, 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. Cost and practicality weigh against this alternative.

Mutual-aid agreements (e.g., Inter-Agency agreements) with other organizations to use their data centers, etc., have tended to be paper agreements which do not work in practice, because they often require that redundant resources and excess capacity exist. However, they can be effective if the involved organizations commit to increasing their respective data processing capacities as part of the agreement.

Cold sites are shells which must be equipped to operate as alternate sites. Since they require a 2-3 week delay while the necessary equipment is installed, cold sites are not likely to be a viable alternative for an organization which 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 AIS facilities which 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. There are usually additional user fees for using the site for testing and/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/Software

Given the rapidity of technological change, hardware compatibility is especially important, because new products tend to compromise the ability of previous products to operate. The industry is often

concerned with upward compatibility. However, in a disaster recovery situation, downward compatibility may become the primary concern, e.g., a critical backup tape stored in a vault has to load properly on the backup system. If the alternate site is a mirror image of the principal site, as is usually the case in a multi-site organization, then hardware is not a factor. In any other approach to contingency planning for large AIS facilities/ITUs, however, hardware and software requirements must be defined to ensure compatibility with the principal site and sufficient capacity to run critical data until recovery is completed.

Hardware includes computers and peripherals. If an online application is deemed critical, then telecommunications equipment is also included. If the organization has decided on a cold site for the alternate site, then the logistics of ordering and installing the hardware must be addressed. If a hot site is selected, the Request for Contract (RFC) to contract for the service must specify the compatibility and capacity requirements of the necessary hardware.

c. Software and Data

Software and data which are critical to the organization's mission must be backed up frequently and maintained off-site from the AIS facility/ITU. These include current operating software, critical applications software, and critical data bases.

The contingency plan must specify the data, how frequently they are backed up, and 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 data processing center (ODPC).

d. Personnel

The contingency plan must specifically identify the personnel designated to run the ODPC, if necessary, until recovery is completed at the principal AIS facility/ITU. This requires a special commitment, as the ODPC is likely to be located a significant distance from the principal AIS facility/ITU.

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 ODPC. Pre-cleared

blanket authorizations may be necessary to move personnel to the ODPC quickly.

e. Operating Procedures

Operating procedures are specific to the ODPC. They are developed and validated during testing at the ODPC.

f. Recovery

Recovery from a disaster is complete when the principal AIS facility/ITU 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 should be a part of the contingency plan and should be maintained off-site. It is advisable to clear procurement paperwork for hardware, AIS facilities, and ITUs as part of the contingency plan, prior to actual need.

Once the AIS facility/ITU has been physically restored, the final step to return to full operation involves transporting the critical operating software, applications data, and personnel from the ODPC back to the principal AIS facility/ITU.

2. Testing the Plan

One recommended strategy for testing the contingency plan is to test each critical application of the AIS facility/ITU individually. In this scenario, the software used to run each application is taken to the ODPC 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 is to run all of them at the test site together. 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 software/ application versions 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 vitally important,

because it is likely that confusion and disorganization would be rampant if and when the requirement to implement the plan arises. It is especially important for designated personnel with specific responsibilities to know who they are and to practice recovery operations in a test situation.

One approach for implementing the plan is a command center. A command center is an office located outside the AIS facility/ITU 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. They could then begin to operate under revised processing procedures and alternate means of handling system input/output, based on the shifting of workloads to the ODPC. 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 and/or be thoroughly briefed on pertinent aspects of it.

E. CONTINGENCY PLANNING PROCESS FOR OFFICE AUTOMATION AND PERSONAL COMPUTER STAND-ALONE UNITS

In contrast to the cost associated with contingency planning for large AIS facilities/ITUs based on mainframe, minicomputers, or Local Area and Wide Area Networks, the cost associated with contingency planning for office automation and personal computer AIS facilities/ITUs is 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 AIS facilities/ITUs.

The main concerns in the contingency planning process for office automation and personal computers are data backup and software backup, with particular emphasis on customized software which is not available from a retail computer store. The cost to replace almost any customized software will exceed the total cost to replace the hardware. The loss or compromise of proprietary data or data subject to Privacy Act provisions can also be costly.

Fortunately, there are integrated operating techniques which allow continuous backup, as opposed to performing discrete backup operations. Streaming is a recommended technique. Streaming involves the use of tape devices with microcomputers to backup and software which are resident on disk.

The contingency plan for an office automation or personal computers should specify where the backed up data and software are stored. They could be stored in a

fireproof office safe, a lockable file cabinet, or a vault, preferably in a location which is not adjacent to the facility. If the cost is justified, they should be maintained off-site. A copy of current operating procedures should also be stored with the data and software.

CHAPTER VII. PERSONNEL SECURITY/SUITABILITY AND TRAINING

A. Overview
B. Responsibilities
C. Requirements

A. OVERVIEW

This chapter presents an overview of the Department's Personnel Security/Suitability Program and how it applies to DHHS' AIS Security Program. DHHS' Personnel Security/ Suitability Program is outlined in detail in Instruction 731-1 of the Department's *Personnel Manual,* see "Personnel Security/ Suitability Policy and Guidance." Instruction 731-1 sets forth Departmental policy in the areas of position sensitivity, suitability for Federal employment, personnel investigations, waivers, access to classified materials, and other personnel security considerations, and deals in detail with the responsibilities of management officials who carry out these functions. Readers should obtain a copy of Instruction 731-1 to ensure full compliance with DHHS Personnel Security/Suitability procedures and requirements. For additional assistance, supervisors can also consult the DHHS "Supervisor's Guide to Personnel."

This chapter also outlines DHHS' Automated Information Systems Security Training and Orientation Program (AIS-STOP). Both the Office of Management and Budget Circular A-130 and the Computer Security Act of 1987 require Departments and Agencies to have AIS security training and orientation programs.

It is important to note that the information in this chapter applies to all DHHS personnel and contractor personnel.

B. RESPONSIBILITIES

Instruction 731-1 of the DHHS *Personnel Manual* lists in detail the responsibilities for personnel security and suitability policy and practices in this Department. These responsibilities are not re-enumerated in this chapter. The responsibili-ties listed below apply to the DHHS AIS Security Training and Orientation Program.

1. Assistant Secretary for Management and Budget (ASMB)

   The ASMB is responsible for overall policy and coordination of the DHHS AIS-STOP Program.

2. Heads of Operating Divisions (OPDIVs) and Regional Directors (RDs)

OPDIV heads and RDs are responsible for:

a. Ensuring that the organizations within their jurisdictions comply with the personnel security provisions of this chapter and Instruction 731-1 of DHHS' *Personnel Manual.*

b. Developing and implementing an AIS security training and orientation program, in accordance with the following requirement from the Computer Security Act of 1987:

> *Each Federal agency shall provide for the mandatory periodic training in computer security awareness and accepted computer security practice of all employees who are involved with the management, use, or operation of each Federal computer system within or under the supervision of that agency.*

3. AIS Managers, AIS Facility Managers, and ITU Managers

AIS Managers, AIS Facility Managers, and ITU Managers are responsible for determining, or assisting in the determination of, the security level designations for all critical and sensitive computer-related personnel positions and for ensuring that all contractor and DHHS personnel within their organizations have the appropriate background suitability checks and AIS security training and/or orientation.

4. Organization Information Systems Security Officer (ISSO)

The ISSO in each DHHS organization is responsible for monitoring the organization's adherence to the DHHS Personnel Security/Suitability Program for computer-related positions and AIS-STOP programs, in conjunction with the OPDIV Senior ISSO or STAFFDIV/RO ISSO.

C. REQUIREMENTS

1. DHHS Personnel Security/Suitability Program

Instruction 731-1 of the *DHHS Personnel Manual* details the requirements for personnel security and suitability policy and practices in this Department; these requirements are not re-enumerated in this chapter. To facilitate understanding of DHHS' four position sensitivity designations and how they may be applied to AIS related positions, we quote below from Instruction 731-1, Section 60 (pages 13-15), "Guidance AIS Positions:"

Guidance AIS Positions (Use only if applicable)

1. *The proliferation of word processors and desk top computers raises questions of computer security. Many of these units stand alone or are linked to one or two like units to form a small automated data system, while others may be linked to a larger AIS but with limited or restricted access to specific parts of the database. In other instances, the employee may have access to a large database without restriction.*

   Generally, any Federal service and contractor position in which the incumbent has a "hands-on" role as a programmer or operator or has access to a mainframe computer, personal computer (PC), minicomputer, or word processors linked to others to form an AIS that allows for data manipulation is a computer-related or AIS position. Designation of position sensitivity for these positions must take into account the nature of information in the AIS database, the uses to which the data is put, control and authentication of individual users, methods or techniques used to augment or enhance protection/safeguarding of AIS information, and physical security safeguards and access controls for the specific AIS.

   Positions that utilize a PC or word processor solely for composing correspondence with no linkage to an AIS are not considered to be "computer-related" or "C" positions.

2. *The four sensitivity levels and the criteria for AIS positions are defined as follows:*

   a. *Special-Sensitive (Level 4C) positions have a potential for INESTIMABLE DAMAGE to the computer security or a significant AIS; requirements are above those at the Critical-Sensitive level*

   b. *Critical-Sensitive (Level 3C) positions have a potential for EXCEPTIONALLY GRAVE DAMAGE to the computer security of a significant AIS. Positions could include those in which the incumbent is responsible for the planning, direction, and implementation of a computer security program; has a major responsibility for the direction, planning, and design of a computer system, including the hardware and software; or can access a*

system during the operation or maintenance stages, with relatively high risk for causing grave damage or realizing significant personal gain. Such positions may involve the following:

(1) Responsibility for the development and administration of major AIS programs and also including direction and control of risk analysis and/or threat assessment

(2) Significant involvement in life-critical or mission-critical systems

(3) Responsibility for the preparation or approval of data for input into a system that does not necessarily involve personal access to the system but with relatively high risk for effecting grave damage or realizing significant personal gain

(4) Relatively high risk assignment associated with or directly involving the accounting, disbursement, or authorization for disbursement from system of (1) dollar amounts of $10 million per year or greater or (2) lesser amounts if the activities of the individual are not subject to technical review by higher authority at the Critical-Sensitive level to ensure the integrity of the system

(5) Major responsibility for the direction, planning, design coding, testing, security maintenance, operation, monitoring, and/or management of systems hardware and software

(6) Hardware maintenance or repairs requiring entry to an AIS facility or access to any part of component of an AIS

(7) Responsibility for administering and operating AIS, the control and functioning of an AIS facility, and the design of programs, or modification or installation of system software

(8) Use of application programs via over-the-counter or remote means and the ability and means to create, destroy, change or retrieve data or program instructions in an AIS.

c. *Noncritical-Sensitive (Level 2C) positions have the potential for SERIOUS DAMAGE to AIS computer security. Positions could include those in which the incumbent is responsible for the direction, planning, design, operation, or maintenance of a computer system, and whose work is technically reviewed by a higher authority at the Critical-Sensitive level to ensure the responsibility for systems design, operating, testing, maintenance, and/or monitoring. This level includes, but is not limited to, the following:*

(1) *Access to and/or processing of proprietary data, information requiring protection under the Privacy Act of 1974, and Government-developed privileged information involving the award of contracts*

(2) *Accounting, disbursement, or authorization for disbursement from system of dollar amounts up to approximately $10 million per year*

d. *Nonsensitive (Level 1C) positions have the potential for PREJUDICIAL DAMAGE to the computer security of a significant AIS; includes all AIS positions not falling into one of the other sensitive levels. For example:*

Positions that input and receive output data which requires no controlled access dissemination.

2. AIS Security Training and Orientation Program (AIS-STOP)

Public Law 100-235, the Computer Security Act of 1987, requires mandatory periodic training for all employees involved in the management or use of Federal computer systems that contain sensitive information. Office of Personnel Management regulation (5 CFR Part 930), entitled "Training Requirement for the Computer Security Act," specifies that:

- The subject matter of the training should stress awareness of the computer system's vulnerabilities and risks and be organized around each Agency's computer security policies, practices, and procedures. The training should provide the knowledge and skills needed to apply these policies, practices, and procedures.

- Training is a continuous process and at a minimum should be provided whenever there is a significant change in the Agency's information security environment or procedures.

- Refresher training, including computer security awareness refresher training, should be provided as appropriate based on the sensitivity of the information.

All DHHS AIS-STOP training should address AIS security practices and procedures for:

- Meeting information security objectives;
- Responsibility and accountability;
- Information accessibility, handling, and storage;
- Physical and environmental hazard protection;
- Systems and data access controls;
- Emergency and disaster situations;
- Identification of threats and vulnerabilities; and
- Other related security matters.

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.

All OPDIVs, ROs, Agencies, and facilities should include security awareness as part of their existing computer training, management courses, and employee orientation. Non-classroom modes of delivery of training are acceptable, e.g., computer assisted training, video tapes, workbooks, job aids, and desk guides.

As stated above, OPDIV heads and RDs are responsible for the development and implementation of an effective AIS-STOP within their organization. AIS-STOP programs should ensure that all DHHS and contractor personnel are aware of their security responsibilities and know how to fulfill them. AIS-STOP programs need to address the training and orientation needs of the following types of DHHS and contractor personnel:

a. Executives

Executives need to be briefed to understand their responsibilities for implementing DHHS' AIS security program, e.g., setting organizational specific policy on the protection of information and processing resources with the broad objectives of ensuring cost-effective confidentiality, integrity, and availability within management judgment

about acceptable levels of risk; assigning responsibilities to competent individuals and holding those individuals accountable; and providing visibility and operating resources for a computer security program.

b. Program and Functional Managers

These managers need to be briefed/trained to understand their role in designating the sensitivity of automated information and the criticality of systems which support their functions, and for ensuring that cost-effective security controls are implemented which will protect data from unauthorized disclosure, modification, or destruction. Functional managers should understand the need/requirements for contingency and disaster recovery planning and for the issuance of security procedures, guidelines, or standards directed toward protecting the daily operations for which they are responsible.

c. IRM, Security, and Audit Personnel

While these Agency officials have different responsibilities and roles depending upon their organizational location, they require extensive training to ensure comprehensive knowledge of the AIS security discipline, as well as DHHS and program AIS security requirements, policies, and procedures. Information systems security officers (ISSOs) need training in the technical aspects of AIS vulnerabilities, risks, techniques, and safeguards. ISSOs should be the experts who develop AIS security policy and guidance, assist with safeguard selection, and evaluate security implementation.

d. ADP Management, Operations, and Programming Staff

These managers and specialists need technical training commensurate with their responsibilities for implementing AIS security policy and for providing security controls to ensure the protection of information and applications. They require technical knowledge to develop and issue procedures, guidelines, or standards that provide guidance and direction, not only for the work flow process of the AIS, ITU, or computer facility but also for the technical and functional support their AIS, ITU, or facility provides to other elements of the Department. They may require specialized training to properly execute their major role in contingency planning and recovery procedures to assure continuity of operations for the critical workload of their organizations.

e. End User Personnel

All users of automated information technology must receive some kind of general AIS security awareness orientation or training. These personnel use computers on a full or part-time basis to perform their jobs. The extent of AIS security training depends on the individual's responsibilities and the sensitivity of information or criticality of systems to be created, automated, and/or accessed. The Department recognizes that almost all DHHS personnel may eventually require AIS security awareness orientation or training, given the rapid growth in the use of office automation (OA) equipment and personal computers (PCs). At a minimum, all employees should receive some initial awareness training, and specific security training should be a part of every subsequent AIS course the employee takes.

f. Contractor Personnel

Contractors need security training commensurate with their responsibilites for performing work under the terms and conditions of their contractual agreements.

CHAPTER VIII. AIS FACILITIES

A. OVERVIEW

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

The Department's AIS 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 AIS facilities which house AIS equipment. These policies and guidelines also apply to Information Technology Utilities (ITUs), since the various components of ITUs are housed in AIS facilities.

Although personal computers and word processors are technically considered to be AIS 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 do not apply to them. (See Chapter X for a full discussion of personal computers and word processors.)

B. RESPONSIBILITIES

1. AIS Facility Managers

   AIS Facility Managers are responsible for:

   a. Specifying, implementing, and reviewing procedures used to protect their facilities/ITUs and operating systems. This involves the performance of risk analyses and the determination of minimum safety requirements and safeguards. The minimum safety requirements and safeguards for all AIS facilities are outlined in Chapter III, Exhibit III-A: Matrix of Minimum Security Safeguards.

   b. Ensuring that their facilities comply fully with the physical security requirements as defined in Part 7 of the *DHHS General Administrative Manual.*

2. Heads of Operating Divisions (OPDIVs) and Regional Directors (RDs)

   OPDIV heads and RDs are responsible for certifying that they have provided the resources required to properly protect the AIS facilities and operating systems within their jurisdictions, commensurate with the determined acceptable level of risk.

C. OPERATING SYSTEMS

Computer operations within DHHS fall into two broad categories: on-line time-sharing operations and sequential batch operations. Most of the technical safeguards required within the AISSP apply to time-sharing operations; however, organizations which use batch operations should also be aware of the requirements, and should apply them where needed.

1. Operating System Requirements

   The requirements for protecting the operating systems of AIS facilities are as follows:

   a. The operating system shall be run using features that guarantee systems integrity and prevent unauthorized use of sensitive system interfaces.

b. The operating system must control access to the data files and software programs stored in the AIS facility. It is recommended that vendor packages specifically designed for this purpose be used (e.g., RACF, Top Secret, and ACF-2).

c. The operating system should record and display non-routine activity that may indicate a security violation (e.g., operator overrides, access failures due to the use of incorrect passwords, and terminal blackouts).

d. The AIS Facility Manager should ensure that the operating system:

(1) Provides safeguards to protect operational status and subsequent re-start integrity during and after shutdown.

(2) Includes complete and current documentation which permits the construction of audit trails for the purpose of tracking non-routine activity.

e. The AIS Facility Manager should ensure the installation of a software feature(s) that will automatically lock-out a terminal if it is not used for a specified period of elapsed time, for a specified period after normal closing time, or if a password is not entered correctly after a specified number of times.

2. Procedural Safeguards

a. There are many possible methods for manipulating batch and on-line systems. Organizations which use such systems must continually evaluate their systems to determine if they can be circumvented and must test their security safeguards to ensure that they are functioning as intended.

b. Individuals may be more likely to misuse AIS capabilities if they act alone. AIS Facility Managers should institute procedures for separating all duties within their AIS facilities. Certain duties should always be separated; for example, scheduling, operating, programming, storage, and library functions.

c. The rules for operators must be specific and complete, and operators must not be permitted to deviate from them. Proper instruction and training must be given to operators to guard against practices such as giving out passwords over the telephone and unlocking terminals by operator override.

d. AIS Facility Managers should establish procedures which require validation of operating systems prior to implementation. Validation should be performed on both new systems and modified systems. The purpose of the validation is to ensure the inclusion of security safeguards prior to implementation.

D. PHYSICAL SECURITY

1. Introduction

In accordance with the Departmental AISSP, all DHHS organizations must implement physical security safeguards to protect the Department's AIS resources. The safeguards must be applied in all administrative, physical, and technical areas. They can be achieved through 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 AIS facilities are outlined in Chapter III, Exhibit III-A: Matrix of Minimum Security Safeguards. AIS Facility Managers must also ensure that their facilities fully comply with the physical security requirements as defined in Part 7 of the *DHHS General Administrative Manual.*

The Matrix of Minimum Security Safeguards is not all-inclusive: it reflects the minimum security requirements that must be implemented until a formal risk analysis of an AIS facility has been conducted. Based on the results of a risk analysis, additional safeguards may be added. A waiver request must be submitted to the Deputy Assistant Secretary for Information Resources Management (DAS/IRM) if an organization cannot, or desires not to, implement specific minimum security requirements for reasons of negative economic or operational impact.

For additional guidance on security safeguards, refer to National Bureau of Standards (NBS) Federal Information Processing Standards (FIPS) Publication 31, "Guidelines for Automatic Data Processing Physical Security and Risk Analysis" and the General Services Administration (GSA) Federal Procurement Management Regulations (FPMRs) 101-35.3 and 101-36.7. For guidance on waiver requests, refer to Chapter IV: AISSP Administration at the Operating Division/ Staff Division/Regional Office (OPDIV/STAFFDIV/RO) Level.

Before selecting and implementing safeguards to protect the physical security of AIS facilities, the AIS Facility Manager should identify the various components of the AIS facility that require protection; for example:

b. The operating system must control access to the data files and software programs stored in the AIS facility. It is recommended that vendor packages specifically designed for this purpose be used (e.g., RACF, Top Secret, and ACF-2).

c. The operating system should record and display non-routine activity that may indicate a security violation (e.g., operator overrides, access failures due to the use of incorrect passwords, and terminal blackouts).

d. The AIS Facility Manager should ensure that the operating system:

(1) Provides safeguards to protect operational status and subsequent re-start integrity during and after shutdown.

(2) Includes complete and current documentation which permits the construction of audit trails for the purpose of tracking non-routine activity.

e. The AIS Facility Manager should ensure the installation of a software feature(s) that will automatically lock-out a terminal if it is not used for a specified period of elapsed time, for a specified period after normal closing time, or if a password is not entered correctly after a specified number of times.

2. Procedural Safeguards

a. There are many possible methods for manipulating batch and on-line systems. Organizations which use such systems must continually evaluate their systems to determine if they can be circumvented and must test their security safeguards to ensure that they are functioning as intended.

b. Individuals may be more likely to misuse AIS capabilities if they act alone. AIS Facility Managers should institute procedures for separating all duties within their AIS facilities. Certain duties should always be separated; for example, scheduling, operating, programming, storage, and library functions.

c. The rules for operators must be specific and complete, and operators must not be permitted to deviate from them. Proper instruction and training must be given to operators to guard against practices such as giving out passwords over the telephone and unlocking terminals by operator override.

d. AIS Facility Managers should establish procedures which require validation of operating systems prior to implementation. Validation should be performed on both new systems and modified systems. The purpose of the validation is to ensure the inclusion of security safeguards prior to implementation.

D. PHYSICAL SECURITY

1. Introduction

In accordance with the Departmental AISSP, all DHHS organizations must implement physical security safeguards to protect the Department's AIS resources. The safeguards must be applied in all administrative, physical, and technical areas. They can be achieved through 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 AIS facilities are outlined in Chapter III, Exhibit III-A: Matrix of Minimum Security Safeguards. AIS Facility Managers must also ensure that their facilities fully comply with the physical security requirements as defined in Part 7 of the *DHHS General Administrative Manual.*

The Matrix of Minimum Security Safeguards is not all-inclusive: it reflects the minimum security requirements that must be implemented until a formal risk analysis of an AIS facility has been conducted. Based on the results of a risk analysis, additional safeguards may be added. A waiver request must be submitted to the Deputy Assistant Secretary for Information Resources Management (DAS/IRM) if an organization cannot, or desires not to, implement specific minimum security requirements for reasons of negative economic or operational impact.

For additional guidance on security safeguards, refer to National Bureau of Standards (NBS) Federal Information Processing Standards (FIPS) Publication 31, "Guidelines for Automatic Data Processing Physical Security and Risk Analysis" and the General Services Administration (GSA) Federal Procurement Management Regulations (FPMRs) 101-35.3 and 101-36.7. For guidance on waiver requests, refer to Chapter IV: AISSP Administration at the Operating Division/ Staff Division/Regional Office (OPDIV/STAFFDIV/RO) Level.

Before selecting and implementing safeguards to protect the physical security of AIS facilities, the AIS Facility Manager should identify the various components of the AIS facility that require protection; for example:

a. Computer room
b. Data control and conversation area,
c. Programmer's area,
d. Terminal/remote job entry (RJE) room,
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 (including cooling towers and water supply),
k. Telephone closet,
l. Power supply area (including transformer vaults and power panels),
m. General office area (where sensitive data is handled).

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

2. Access Control

The AIS 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

Equip all doors in all areas containing AIS 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 AIS 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, and require an escort for them at all times.

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

(4) Limit the presence of cleaning and maintenance personnel to the period when regular employees are on duty. This must be coordinated with the building manager.

(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 AIS facilities, remote job entry facilities, terminal rooms, library, or media storage areas left unlocked after-hours.

(6) Post "For Authorized Personnel Only" signs where sensitive data is used or stored.

3. Protection of Sensitive Materials

All DHHS organizations should establish procedures to control the handling, distribution, storage, disposition, and destruction of materials which contain sensitive data. The AIS 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 Level 3 and 4 sensitive materials, such as data printouts and other hard copy materials, software documentation, operating manuals, and handbooks, are labelled 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 user management maintains a retention schedule and a monitoring procedure for all data in the AIS facility, in consultation with the organization's records management officer.

(3) 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.

(4) Protect sensitive data during an external evaluation.

4. Facility Construction

OPDIV/STAFFDIV/RO security representatives, along with a representative from the Department, must review the construction plans for all new AIS facilities and the modifications to existing AIS facilities to determine the most cost-effective method for securing the facilities, given their vulnerability to penetration by outside forces, the sensitivity of the data to be processed, and the value of the equipment to be protected.

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

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

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

c. The most desirable location to house AIS equipment is in an interior room, above the first floor, having four solidly-constructed walls which extend from the true floor to the true ceiling. This is particularly important it the AIS equipment will not be attended on a 24-hour basis. Attended AIS equipment requires only a minimum level of

protection, since unauthorized access is easily detected by resident personnel.

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 AIS facility is a potential target for vandalism, windows should be barred, screened, or opaqued.

5. Fire Safety

OPDIV/STAFFDIV/RO security representatives, along with a representative from the Department, should ensure that appropriate safeguards are implemented to prevent, detect, and/or suppress fires and protect AIS 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 75-1981, Protection of Electronic Computer/Data Processing Equipment, and local ordinances and building codes.

a. Fire Prevention

Take preventive measures to minimize the threat of fires, such as keeping AIS equipment rooms clear of trash and unnecessary supplies and prohibiting smoking.

b. Fire Detection

Install smoke and/or fire detection equipment within the AIS facility to ensure early detection of fires. Connect all alarms to a central alarm within the AIS facility and to a manned guard station or fire station, if feasible.

c. Fire Suppression

Install fire suppression equipment; for example, overhead sprinkler systems with protected control valves and hand-held fire extinguishers. CO_2 extinguishers should be used in AIS equipment areas, and pressurized water extinguishers used in paper storage, media library, and other similar areas.

d. Fire Emergency Response

(1) Provide equipment for emergency power shutdown and air conditioning in the event of fire or other emergencies, and provide that overhead lighting is not shut down. Provide covers or other protective measures for emergency power controls and fire alarm switches to prevent accidental activations.

(2) Equip air-conditioning and duct-work systems with dampers to prevent the spread of fire, smoke, or chemical agents. Smoke exhaust systems are recommended for all AIS operations areas to minimize the potential hazard to personnel, AIS equipment, and storage media.

(3) Place waterproof sheets strategically throughout the AIS facility to prevent or minimize the effects of water damage.

(4) Develop a fire emergency preparedness and evacuation plan. The plan should include the training of fire emergency response teams and should include on-site orientation visits for the local fire department. Develop and test the fire emergency preparedness and evacuation plan and conduct fire drills at least annually.

CHAPTER IX. APPLICATION SYSTEMS AND DATA SECURITY

A. OVERVIEW

This chapter presents the Automated Information Systems Security Program (AISSP) policy for determining the sensitivity of automated data files and the operational criticality of automated application systems. The requirements contained in this chapter apply to all DHHS organizations which use automated information systems and automated data files. Organizations should use the guidance presented in this chapter to ensure the security of their Automated Information Systems (AISs).

The Department presumes that all of the data which are collected, maintained, and processed by an organization have some value. However, since neither all data nor all data applications are of equal value nor have equal sensitivity to an organization, they need to be categorized and protected according to their degree of value and sensitivity. Data files and application systems which are categorized with high security level designations require more stringent security safeguards than those with low security level designations. Data files and application systems which are categorized at the lowest end of the spectrum usually require only minimum precautions.

B. RESPONSIBILITIES

1. Heads of Operating and Staff Divisions (OPDIV/STAFFDIVs) and Regional Directors (RDs)

   OPDIV/STAFFDIV heads and RDs are responsible for ensuring that all application systems and automated data files within their jurisdictions are identified and that an Application System Manager is appointed for each application system and that a Data File Manager is appointed for each data file.

2. Application System Managers and Data File Managers

   Application System and Data File Managers are responsible for developing, implementing, and reviewing procedures to protect the integrity of the application system/data file for which they have responsibility. Application System/Data File Managers are also responsible for:

a. Notifying the organization Information Systems Security Officer (ISSO) and users of the level of security required by their application systems/data files.

b. Certifying that the security requirements of their application systems/data files are being met or will be met.

c. Documenting individual security requirements or Risk Assessment recommendations that cannot be met.

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

e. Ensuring that their application systems/data files are only run at AIS facilities and Information Technology Utilities (ITUs) that are certified at a level of security equal to or higher than the security level designated for their application systems/data files.

3. OPDIV Senior and STAFFDIV/Regional Office (RO) Information Systems Security Officers (ISSOs)

OPDIV Senior ISSOs and STAFFDIV/RO ISSOs are responsible for maintaining an inventory of the security level designations for all application systems and data files within their organizations.

4. Users

Users are responsible for using the security safeguards required to protect application systems/data files. Users are also responsible for:

a. Assisting Application System/Data File Managers in determining the required security levels for application systems/data files.

b. Running application systems/data files only at AIS facilities and ITUs that are certified at a level of security equal to or higher than the security level designated for their application systems/data files.

c. Using all of the security measures available to protect application systems and data files.

C. APPLICATION SYSTEMS AND DATA MANAGEMENT

1. Requirements

The primary responsibility for application system and data file management is at the OPDIV/STAFFDIV head and RD level. Specifically, OPDIV/STAFFDIV heads and RDs are required to:

a. Ensure that an Application System Manager is assigned for each application system and a Data File Manager is assigned for each data file for all application systems/ data files within their jurisdictions.

b. Ensure that each application system and data file within their jurisdictions is assigned a security level designation of 1, 2, 3, or 4. (See Chapter II: Security Level Designations for the definitions of the four criticality security levels for application systems and the four sensitivity security levels for data files.)

c. Ensure that required security safeguards are in place for all application systems and data files within their jurisdictions. (See Exhibit IX-A: Application System/Data File Security Safeguard Matrix for the minimum required security safeguards for application systems/data files.)

d. Ensure that each application system within their jurisdictions has a certified security status. (See Exhibit IX-B: Application Systems Security Certification/Accreditation.)

e. Document the rationale for those security requirements or recommendations cited in Risk Assessments and\or Computer System Security Plans which have not or cannot be implemented.

2. Application System and Data File Security Level Designations

Application System and Data File Managers should assign security level designations to their application systems/data files using the definitions provided in Chapter II: Security Level Designations. The security level designations determine the minimum security safeguards required to protect their application systems/data files. For the most part, application systems/data files will fit one of the four levels of operational criticality/data sensitivity. However, if an application system/data file has a range of possible security level designations, the Application System/Data File Manager should

make the overall security level determination for the application system/data file based on knowledge of the operational criticality of the application system or the data sensitivity of the data file. Exhibit III-A: Matrix of Minimum Security Safeguards outlines the minimum security safeguards required for each security level.

It is important to emphasize that an application system/ data file may only run at an AIS facility/ITU that is certified at an equal or higher security level, and that the Application System/Data File Manager is responsible for ensuring that all application system/data file users use all of the required safeguards for the application system/data file.

3. Data Exchange

Data received from one department, agency, or organization for use by another department, agency, or organization must carry the security level designation assigned by the owner. For example, Department of Defense (DOD) or Social Security Administration (SSA) data which are used by another Federal department, agency, or organization must carry the DOD or SSA security designation, and be protected accordingly.

D. APPLICATION SYSTEM CERTIFICATION/ACCREDITATION

FIPS Pub 102, Guideline for Computer Security Certification and Accreditation, states:

> *Certification consists of a technical evaluation of a sensitive application to see how well it meets its security requirements.*
>
> *Accreditors use the certification report to help evaluate certification evidence. They then decide on the acceptability of application security safeguards, approve corrective actions, insure that corrective actions are implemented, and issue the accreditation 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 certification process must begin during the design and development stages. Sensitive application systems must be recertified at least once every three years. Every sensitive application system must be recertified if the safeguard requirements outlined in this Handbook change, the system is violated, or the system undergoes a significant modification.

The Computer System Security Plan is the central element of the certification and accreditation process for sensitive systems. The CSSP can function as the certification report since its four basic sections (System Identification, Sensitivity of Information, System Security Measures, and Additional Comments) are designed to cover the major security elements of a system.

The accrediting official should review the following documents, at a minimum, in the accreditation process for a sensitive application:

Computer System Security Plan
Security Specifications and Test Results
Contingency Plan
Other pertinent documents (e. g., risk analyses, audits, OIRM reviews)

When the accrediting 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 Accrediting Official completes three copies of Exhibit IX-B: Application System Security Certification/ Accreditation to document the certification procedure.

2. The Application System Manager retains one copy of the security certification form and forwards one copy of the certification form to the OPDIV Senior ISSO. The third copy may be retained for central files, etc.

3. Applications which do not meet procedural or substantive security requirements should not be certified. In such cases, complete the statement Deferral of Certification/Accreditation. The deferral statement includes a list of deficiencies which must be remedied. When a Deferral of Certification/Accreditation statement is executed, the application must be reported as a security weakness under the A-123 reporting process.

Note: The Accrediting Official may be the Application System Manager. However, FIPS Pub 102 states: The more sensitive the application, the higher the management level of the Accrediting Official.

EXHIBIT IX-A: APPLICATION SYSTEM/DATA FILE SECURITY SAFEGUARD MATRIX

Explanation: This matrix provides guidance for identifying the minimum required security safeguards for automated application systems and data files.

Directions: (1) Locate the security level designation of the application system/data file in the left-hand column. (See Chapter II: Security Level Designations for the definitions of the four criticality security levels for application systems and the four sensitivity security levels for data files.) (2) Scan the Xs and Os to the right of the security level designation. An X means that the security safeguard listed above is a requirement and an O means that the security safeguard is optional.

	Security Safeguards					
Security Level	Access Controls	Encryp-tion	Backup Copies	Audit Trails	Periodic Risk Analysis/ Review	Physical Security
4	X	X	X	X	X	X
3	X	O	X	X	X	X
2	X	O	X	O	X	X
1	O	O	O	O	O	O

EXHIBIT IX-B: APPLICATION SYSTEM SECURITY CERTIFICATION/ACCREDITATION

I have carefully reviewed the attached 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 remaining 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 Accrediting Program Official)

EXHIBIT IX-C: DEFERRAL OF CERTIFICATION/ACCREDITATION

Based on a review of the attached system security plan, requirements set forth in OMB Circular A-130, and the security requirements of (name of system), this application cannot be accredited at this time. The reasons for deferring such accreditation include:

[ ] 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 _____

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

(corrective actions)

_____
(Signature/Title of Accrediting Program Official)

CHAPTER X. PERSONAL COMPUTERS AND WORD PROCESSORS

A. OVERVIEW

This chapter presents the Automated Information Systems Security Program (AISSP) policy for protecting personal computers (PCs), word processors (WPs), and their application systems and data from damage, destruction, or misuse. The requirements of this chapter apply to all organizations which use PCs and WPs. Additional requirements apply for PCs/WPs which:

- Use software developed by the user;
- Communicate with other PCs/WPs.

This policy also applies to PCs/WPs owned by DHHS and taken home by DHHS employees, and PCs/WPs owned by DHHS employees and used to accomplish official work. PCs/WPs used in a laboratory environment as part of automated scientific instrumentation are excluded from the policy.

Before PCs/WPs were introduced in the general office environment, the mainframe computer was the principal source of automated data processing (ADP). Now, because almost every PC/WP contains technology which permits local storage and higher order functions such as sorting, list processing, and computation capabilities, many of the security concerns associated with mainframe computers are applicable in the general office.

PC/WP hardware is particularly vulnerable to fluctuations in electrical power, static electricity, and dust. Protecting and safeguarding PC/WP software and data may be even more important, however. Since PCs/WPs are generally easy to access, this can be a difficult problem. Therefore, under Federal regulations, and subject to penalties, all Application System Managers, supervisors, and PC/WP users are responsible for taking actions to safeguard and prevent the improper use of, damage to, or destruction of the data, application systems, and hardware of PCs/WPs. The extent of these actions should be commensurate with the sensitivity of the data, operational criticality of the application systems, and value of the hardware of each PC/WP.

B. GENERAL RESPONSIBILITIES

1. Application System Manager

The Application System Manager is responsible for designating the security level of his/her application system and establishing and communicating the security safeguards required for protecting the application system, the PCs/WPs which run the application system, and the data processed by the application system. He/she is responsible for meeting the requirements listed in Exhibit X-A: AIS Security Checklist for Personal Computers and Word Processors. The Application System Manager is usually the lowest level supervisor responsible for PCs/WPs and the staff assigned to use them and can be the same person as the PC user.

2. Users

PC/WP users are responsible for implementing specified security safeguards to prevent fraud, waste, or abuse of the hardware, application systems, and data of the PCs/WPs they are authorized to use.

3. Organization Information Systems Security Officer (ISSO)

The organization ISSO is responsible for assisting the Application System Manager in establishing, and users in implementing, the appropriate security safeguards required to protect PC/WP hardware, application systems, and data from improper use or abuse.

C. SPECIFIC REQUIREMENTS

1. Specific Requirements for Application Systems

a. The Application System Manager must conduct a risk analysis which documents the dollar value of the assets, nature and likelihood of threats against the assets, and effectiveness of existing or proposed security safeguards required to protect the assets of PCs/WPs which run his/her application system.

b. The Application System Manager must establish controls for handling the data processed by his/her application system, such as labeling reports and diskettes, to prevent unauthorized access to or loss of the data.

c. The Application System Manager must develop and maintain a list of persons authorized to access his/her application system and the data it processes.

d. The Application System Manager must ensure that appropriate security safeguards are in place for his/her application system prior to implementation. This requirement applies to all new and all modified application systems.

e. The Application System Manager must provide a user awareness program for the users of his/her application system which provides orientation to established Automated Information System (AIS) safeguards, security problems, responsibilities, procedures, and governing copyright laws and restrictions. AIS security should, at a minimum, be addressed as part of every training course.

f. The Application System Manager must create a backup copy of proprietary software, when authorized by copyright law or software licensing agreements.

g. The Application System Manager must maintain a complete and current set of documentation which describes the application(s), procedure(s), and process(es) for all software utilized by his/her application system.

h. Users must backup automated data files on a periodic basis.

i. Users must ensure that passwords used to access application systems are not accessible.

j. Users and the Application System Manager must periodically reevaluate the adequacy of the security safeguards used to protect the application system. These reevaluations are especially important following changes such as personnel turnover and the installation of telecommunications capabilities on PCs/WPs which run the application system.

2. Specific Requirements for Equipment

a. The Application System Manager must determine the need to install devices to control physical access to or prevent the theft of PCs/WPs which run his/her application system.

b. The Application System Manager must install devices to protect the PCs/WPs which run his/her application system from power fluctuations, surges, and spikes which could lead to unpredictable or undesirable results, such as damage to hardware, the creation of erroneous data, or the loss of data.

c. The Application System Manager, in conjunction with the users of PCs/WPs which run his/her application system, should consider the need for and development of a contingency plan(s). The contingency plan(s) should address emergency operations and recovery procedures in the event that the PCs/WPs which run his/her application system become inoperable for a period of time. The contingency plan(s) could entail the use of alternate PCs/WPs located elsewhere or the use of PC/WPs loaned from a vendor. (See Chapter VI, E: Contingency Planning Process for Office Automation and Personal Computer AIS Facilities/ITUs.)

3. Specific Requirements for Externally-Developed Software

a. The use of software purchased by the Government is governed by the terms and agreements established by the software vendors and the DHHS 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 Departmental procurement policies. Infringement of software copyrights may constitute theft.

b. PC software products may not be copied except to 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 one lawfully must be held accountable for their actions.

c. Application managers purchasing software packages protected by quantity licenses must ensure a tracking system is in place to control the copying and distribution of the proprietary software.

d. Recent incidences of computer viruses within DHHS and elsewhere indicate the need to use prudent practices to prevent the introduction of malicious software into the workplace. Application managers must forbid the use of software downloaded from bulletin

boards. Only shrink-wrapped software or certified shareware should be used.

4. Special Considerations for Sensitive Data

The application systems which are run on most PCs/WPs do not provide data security. This is true for application systems which run on both stand-alone and multi-user PCs/WPs. In most cases, security controls are not required for application systems which run on PCs/WPs. However, if an application system processes sensitive data, lack of security controls can be a distinct vulnerability. Therefore, whenever sensitive data are processed by an application system on a PC/WP, the following administrative controls must be implemented by users and/or the Application System Manager to ensure adequate security of the data.

a. Users must ensure that diskettes which contain sensitive data are only accessed by persons with a clear "need to know" and a security level clearance equal to or higher than the security level designation of the data. Users must also ensure that diskettes which contain sensitive data (i.e., data rated at Levels 2, 3, or 4) are labeled with the words "This diskette contains SENSITIVE INFORMATION."

b. Users should not normally store both sensitive and non-sensitive data files on the same diskette. If a diskette contains data files with different security level designations, the diskette as a whole assumes the security level designation of the data file with the highest designation.

c. Users must ensure that diskettes which contain sensitive data are stored in key or combination locked files, cabinets, or desks, as appropriate for the type of data they contain, when not in use.

d. Users must ensure that printer ribbons, as appropriate, are marked in accordance with the security requirements of the data they were used to produce. Printer ribbons used to produce sensitive data should be stored in a key or combination locked cabinet.

e. Users must not leave PCs/WPs unattended when processing sensitive data or when sensitive data or a critical application system is resident in memory.

f. The Application System Manager must ensure that the hardware components of PCs/WPs that run his/her application system are

physically located and positioned to preclude unauthorized persons from viewing their display or output. Hardware components include terminals, printers, and cathode ray tubes (CRTs).

g. Only personnel authorized by the Application System Manager are allowed to access PCs/WPs which run his/her application system.

h. Multi-user PCs/WPs should only be located in offices which can be secured by approved locks when unoccupied. One alternative is the installation of a Central Processing Unit (CPU) KEYLOCK feature on these PCs/WPs. Other alternatives are data encryption and/or the use of passwords.

i. Diskettes and other magnetic storage media which contain sensitive data may be reused when they are no longer needed to store the data, only after being reformatted, overwritten, or degaussed.

EXHIBIT X-A: AIS SECURITY CHECKLIST FOR PERSONAL COMPUTERS AND WORD PROCESSORS

Explanation: The following questions highlight the AIS security requirements for application systems which run on personal computers (PCs) and/or word processors (WPs). 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, including the value of hardware and software?		
2. Are reports and diskettes properly stored in a security 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 PC or WP, as well as in AIS security requirements?		
5. Are application system access passwords available only to authorized users?		
6. Are the passwords changed when authorized employees leave DHHS?		
7. When changes are introduced (e. g., new applications, personnel turnover, tele-communications) are risks re-examined?		
8. Are data files backed up periodically? 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?		

REQUIREMENT	YES	NO
12. Are there special devices such as cipher locks or anchor pads installed to lessen the risk of theft or unauthorized access to the PC or WP?		
13. Are surge suppressors installed?		
14. In the event that the PC or WP is unavailable for a period of time, is a contingency plan in place?		
15. Are sensitive data stored or processed on the PC or WP? (If the answer is "yes", proceed to question 16.)		
16. Have the personnel who use the PC or WP obtained appropriate security clearances?		
17. Has password protection capability been implemented to protect the application system? To protect data files?		
18. Are the data encrypted?		
19. Are reports and diskettes specially labelled and controlled?		
20. Are unneeded sensitive reports shredded and unnecessary files written over?		

NOTE: Individuals who conduct AIS security reviews may request specific documentation in support of your responses.

_____ _____
(Signature of Application System Manager) (Date)

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

CHAPTER XI. DATA COMMUNICATIONS

A. OVERVIEW

This chapter presents the Departmental policy for protecting sensitive data which are transmitted by electrical, electro-mechanical, or wave energies. The policy applies to all DHHS 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.

B. POLICY

Every DHHS organization must identify its sensitive electronic data and provide effective and appropriate protection for the data when they are transmitted by data communications equipment. The Information Systems Security Officer (ISSO) and telecommunications and/or data communications officials in the organization must provide needed assistance. This assistance includes:

1. Ensuring that data communications controls and safeguards are operating in support of each application system and/or Automated Information System (AIS) which uses data communications.

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

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

4. Identifying and implementing required changes in the controls and safeguards as needs and technologies change.

All of these actions, and other actions taken with respect to data communications, must adhere to the guidelines and policies issued under National Security Decision Directive No. 145 (NSDD-145), National Policy on Telecommunications and Automated Information Systems Security.

C. RESPONSIBILITIES

AIS Managers, AIS Facility Managers, and Information Technology Utility (ITU) 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 the individuals, then the Agency head designates the individual who has responsibility for the particular equipment and software. Each of the above individuals is responsible for the following:

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

   a. Shows the front-end processor configuration;

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

   c. Indicates transmission speeds and software protocols.

2. Conducting a risk analysis and associated cost-benefit analysis to determine cost-effective and essential security safeguards required to protect the data communications network. The risk analysis should consider all potential risks and all potential safeguarding expenses. The cost-benefit analysis should be based on the risk analysis and on an inventory of the equipment, equipment capabilities, personnel functional abilities, and applications systems used within the network. (See Chapter V: Risk Management.)

3. 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. (See Chapter VI: Contingency Planning.)

4. Establishing and implementing required and appropriate procedures, controls, and security safeguards for the data communications network, as indicated by risk analysis and approved by the Agency head. (See Exhibit XI-A: Matrix of Data Communications Vulnerability for guidance in determining the appropriate security level designation for a data communications network.)

5. Conducting periodic internal control reviews of the security of the data communication network. (See Chapter IV: AISSP Administration at the OPDIV/STAFFDIV/RO Level.)

EXHIBIT XI-A: MATRIX OF DATA COMMUNICATIONS VULNERABILITY

Explanation: This matrix provides guidance for determining the appropriate security level designation for a data communications network. After determining the security level designation using this matrix, refer to Exhibit III-A: Matrix of Minimum Security Safeguards to identify the security controls required to safeguard the network.

IF UNAUTHORIZED ACCESS OR DISRUPTION OF COMMUNICATIONS COULD...	THEN THE SECURITY LEVEL DESIGNATION OF THE NETWORK SHOULD BE...
Cause inconvenience or embarrassment	**Level 1** Low or no Sensitivity/Criticality
Cost the Government $_____	**Level 1-3** Low to High Sensitivity/Criticality (dependent on the dollar amount)
Prevent the Government from carrying out some part of its mission	**Level 1-3** Low to High Sensitivity/Criticality (dependent on the affected aspects of the mission)
Cause harm to or provide unfair advantage to a private entity	**Level 3** High Sensitvity/Criticality
Harm national security	**Level 4** High Sensitivity/Criticality National Security

CHAPTER XII. ACQUISITIONS AND CONTRACTS

A. OVERVIEW

In accordance with the requirements of the Departmental Automated Information Systems Security Program (AISSP), every Request for Proposal (RFP) which involves the development of an Automated Information System (AIS), or the use of Departmental AIS resources, must include appropriate security requirements. Contractors who perform direct AIS services for DHHS, including time-sharing service contractors, are required to meet these requirements. The requirements also apply to contractors who participate in the design, development, operation, and/or maintenance of AIS telecommunications systems for DHHS. All contractors are required to safeguard the Department's application systems, software packages, personal data, sensitive data, trade secrets, and other Departmental AIS assets against destruction, loss, or misuse.

This chapter describes the AISSP policy for establishing the security requirements for solicitations and contracts. All Departmental personnel who award Government monies for AIS services must adhere to the policy guidelines presented in this chapter, whether the services are procured by DHHS or the General Services Administration (GSA).

B. GRANTS AND COOPERATIVE AGREEMENTS

Grants and cooperative agreements are excluded from the policy described in this chapter. However, where appropriate, awarding officials should encourage grantees and cooperative agreement recipients to implement adequate AIS security safeguards.

C. SECURITY STANDARD

All contractors who are involved in developing AISs for use by DHHS, or in providing any other type of service for the Department in which AIS resources are used, must agree to comply with the requirements of the Departmental AISSP. DHHS policy requires that the use or acceptance of Federal contract funds entails

an obligation to properly safeguard all sensitive data, privacy information, and AIS resources.

D. ROLES AND RESPONSIBILITIES

1. Project Officer

Whenever a contract involves the development of an AIS or the use of AIS resources, the awarding DHHS organization must designate a Project Officer to oversee the award and the performance of the contract. The Project Officer may be an Application System Manager, AIS Manager, AIS Facility Manager, or Information Technology Utility (ITU) Manager. The Project Officer is responsible for:

a. Specifying the security requirements for inclusion in the Statement of Work (SOW) in the RFP.

b. Certifying that the SOW complies with the requirements of the Departmental AISSP (see Exhibit XII-A: Solicitation Certification) and obtaining the signature of the organization Information Systems Security Officer (ISSO) on the certification statement.

c. Reviewing proposals received in response to the RFP, and determining which proposals successfully meet the security requirements specified in the SOW.

d. Conducting a technical review of successful proposals with his/her peers, and developing technical evaluation reports on these proposals.

e. Certifying that successful proposals comply with the requirements of the Departmental AISSP (see Exhibit XII-B: Pre-Award Certification) and obtaining the signature of the organization ISSO on the certification statements.

2. Application System Managers/AIS Managers/AIS Facility Managers/ITU Managers

Relevant Application System Managers/AIS Managers/AIS Facility Managers/ITU Managers work with the Project Officer, Contracting Officers, and organization ISSO to ensure that RFPs pertaining to their application systems/ AISs/AIS facilities/ITUs comply with the Departmental AISSP. These managers, as appropriate, also participate in the technical review

conducted by the Project Officer of successful proposals received in response to RFPs.

3. Organization Information Systems Security Officer (ISSO)

The ISSO in the awarding organization assists the Project Officer and appropriate Application System Managers/AIS Managers/AIS Facility Managers/ITU Managers to carry out the provisions of the AISSP policy for solicitations and contracts. The ISSO assistance includes:

a. Providing help, as needed, in drafting the Statement of Work (SOW). If the SOW is for the development of an application system the ISSO will ensure that the appropriate applications security requirements are included in the SOW, e.g., provisions for security specifications, design and testing requirements, and certification procedures. (See XII-E, Statement of Work [SOW] Preparation).

b. Reviewing and signing Agency Procurement Requests as well as the Solicitation Certifications and Pre-Award Certifications included as Exhibits XII-A and XII-B, respectively. For example, the organization ISSO confirms, with his/ her signature on the Pre-Award Certification, that the successful proposals received in response to an RFP and certified by the Project Officer comply with the requirements of the Departmental AISSP.

4. Contracting Officers

Contracting Officers are responsible for taking the following actions on procurements which involve the development of an AIS or the use of AIS resources:

a. Ensuring that the pre-award certification statements of AIS security requirements for successful proposals are signed by both the Project Officer and organization ISSO and submitted with the proposals (see Exhibit XII-B: Pre-Award Certification). The Contracting Officer is prohibited from initiating action on a proposal until a properly executed certification statement is received.

b. Including a statement in the RFP requiring offerors to present a detailed outline of their present or proposed AIS security program in their proposals.

c. Including a statement in the RFP that offerors are required to comply with the SOW in the RFP and with the requirements of the Departmental AISSP (see Exhibit XII-C: Security Policy Statement for Inclusion in Automated Information Systems Contracts). The statement should read substantially as follows:

> The Contractor agrees to comply with the AIS security requirements set forth in the statement of work and applicable portions of the *DHHS AISSP Handbook*. The Contractor further agrees to include this provision in any subcontract awarded pursuant to this prime contract.

d. Furnishing copies of this *Handbook* when requested by offerors who respond to the RFP.

e. Forwarding any forms to the organization ISSO which the winning contractor must submit to verify or obtain personnel security clearances for his/her staff. If the winning contractor does not hold appropriate security clearances for his/her personnel, then the awarding organization is responsible for sponsoring the contractor to obtain the required personnel clearances prior to commencement of the contract work. The costs of the security clearances shall be borne by the awarding organization and reimbursed by the contractor.

f. Ensuring that the technical evaluation reports developed on successful proposals by the Project Officer and his/her peers either detail any AIS security deficiencies or confirm contractor compliance with the requirements.

E. STATEMENT OF WORK (SOW) PREPARATION

1. OMB Circular A-130 states:

Agencies shall assure that appropriate technical, administrative, physical, and personnel security requirements are included in specifications for the acquisition or operation of information technology installations, equipment, software, and related services, whether procured by the agency or by GSA. These security requirements shall be reviewed and approved by the management official responsible for security at the installation making the acquisition.

2. FIRMR, Part 201-39, 1001-1, provides the following specifications for security of information resources, as appropriate:

a. Agency rules of conduct that a contractor shall be required to follow.

b. A list of the anticipated threats and hazards that the contractor must guard against.

c. A description of the safeguards that the contractor must specifically provide.

d. The security standards applicable to the contract.

e. A description of the test methods, procedures, criteria, and inspection system necessary to verify and monitor the operation of the safeguards during contract performance and to discover and counter any new threats or hazards.

f. A description of the procedures for periodically assessing the security risks involved.

g. A description of the personnel security requirements.

h. Consistent with the guidelines for Federal computer security training issued by the National Institute of Standard Technology (NIST) and regulations issued by the Office of Personnel Management (OPM), a description of the security training that the contractor is required to provide to its employees.

i. Consistent with guidelines issued by the Office of Management and Budget (OMB) in the OMB Bulletins [on security], a description of the plan the contractor must develop or follow to provide for the security and privacy of FIP [Federal Information Processing] resources the contractor is required to operate.

3. Security Level Determination

The SOW in the RFP must include appropriate AIS security requirements. The security requirements should be determined by using this *Handbook* and should be based on the technical requirements of the contract. The security requirements should substantiate an overall security level designation which is commensurate with the value and sensitivity/criticality of the AIS resources or services to be provided by a contractor.

Consult the following *Handbook* chapters in determining the security level designation for the SOW in the RFP:

Chapter I - AIS Security Program
Chapter II - Security Level Designations
Chapter III - Security Level Requirements
Chapter VII - Personnel Security, Suitability, and Training
Chapter VIII - AIS Facilities
Chapter IX - Application Systems and Data Security
Chapter X - Personal Computers and Word Processors
Chapter XI - Data Communications

4. Documentation Requirements

The AIS security requirements set forth in the RFP must be sufficiently detailed to enable offerors to easily understand what is required. A general statement that the offeror must agree to comply with applicable requirements is not acceptable. In addition to the security level designation, the SOW in the RFP must contain the following:

a. A list of the minimum security requirements and minimum security safeguards required by the contract and commensurate with the security level designation.

b. The following special provisions to address contractor employees associated with the project:

(1) "Persons without required security clearances cannot perform any contract work."

(2) "Persons without necessary clearances will not have access to project data."

(3) "All contractor personnel designated as Level 4C, 3C, or others as deemed necessary, who are directly performing the work, must be named in the contract and must be subject to a key personnel clause."

(4) "Violation of any of these conditions may lead to termination of the contract."

c. A request that offerors include a copy of their standard security policy and practices in their proposals to address the following:

(1) A description of the facility(-ies) they will be using during the project, and the security of the facility(-ies).

(2) The procedures for handling or accessing Government data and other AIS resources during performance of the project.

(3) The physical storage procedures to protect Government data and other AIS resources during performance of the project.

(4) Any required limitations on employees concerning the reproduction, transmission, or disclosure of data and project information (see Exhibit XII-D: Commitment to Protect Privileged Information Contractor Agreement).

(5) Any required time-sharing procedures employees must follow during performance of the project, if applicable.

(6) Procedures for the destruction of source documents and other related waste material.

d. A request that the offeror acknowledge understanding of the security requirements detailed in the SOW.

e. A request that the offeror acknowledge understanding of the requirement that the Project Officer approve the use by the contractor of any subcontractors, vendors, or suppliers prior to their use.

f. A request that the offeror provide a copy of his/ her organization chart which shows the proposed designation of each personnel position as Level 4C, 3C, 2C, or 1C, as applicable.

g. A request that the offeror provide a brief description of the responsibilities of each position on his/her organization chart, so that the personnel security designations can be evaluated.

h. Copies of the following forms for the certification of contractor employees by the DHHS Office of the Assistant Secretary for Personnel Administration (ASPER):

(1) Standard Form 86, "Security Investigation Data for Sensitive Positions."

(2) Office of Personnel Management (OPM) Form 392A, "Release for General Purposes."

(3) Standard Form 8, "Finger Print Form."

F. PROCEDURE FOR PROPOSAL REVIEW AND CONTRACT AWARD

The procedure for reviewing proposals received in response to the RFP and for awarding the contract for services is as follows:

1. The Contracting Officer forwards the Automated Data Processing (ADP) security components of each proposal to the Project Officer and/or organization ISSO for review and evaluation.

2. The Project Officer and organization ISSO determine that all of the security requirements listed in the SOW for the contract are addressed in the proposal.

3. The Project Officer conducts a technical review of the proposal with his/her peers to determine the adequacy and capability of the contractor to meet the security requirements listed in the SOW for the contract.

4. The Project Officer develops a technical evaluation report on the proposal.

5. The Project Officer and organization ISSO certify that the proposal complies with the security requirements specified in the SOW and the requirements of the Departmental AISSP (see Exhibit XII-B: Pre-Award Certification) and attach the technical evaluation report to the certification.

6. The Project Officer and/or organization ISSO conduct an on-site inspection of the offeror's facility(-ies), if required, to ensure that the facility(-ies) has safeguards commensurate with the sensitivity of data and value of assets to be protected during performance of the contract.

7. The Project Officer provides written confirmation to the Contracting Officer that required security safeguards are in existence at the offeror's facility(-ies). Thereafter, the Contracting Officer may award the contract. The Contracting Officer should include a policy statement similar to Exhibit XII-C: Security Policy Statement for Inclusion in Automated Information Systems Contracts in the contract.

G. INCUMBENT CONTRACTS

Contract Officers and Project Officers must negotiate reasonable time frames for existing contractors to comply with the policy presented in this chapter. As a first step, existing contractors should be required to comply with applicable personnel security requirements. All personnel who directly perform contract work must have an appropriate security clearance. Incumbent contractors are responsible for reimbursing the Department for the cost of investigations. Contracting Officers should forward contractor requests for clearance of incumbent personnel upon receipt to:

Assistant Director
Executive Personnel and Employee Development
DHHS 523-B, HHH Building
200 Independence Avenue, S.W.
Washington, DC 20201

H. CONTRACT ADMINISTRATION

After a contract has been awarded, the Project Officer, organization ISSO, and relevant Application System Managers/AIS Managers/AIS Facility Managers/ITU Managers, in coordination with the assigned Contracting Officer, must conduct periodic reviews of the project to ensure continued compliance with the Departmental AISSP. All instances of noncompliance must be reported to the Contracting Officer, or his/her designated representative, for necessary action.

I. RELATED AUTHORITIES

Code of Federal Regulations (CFR) 45, Part 74 establishes uniform administrative requirements as well as cost principles for DHHS grants and cooperative agreements. It requires the recipients of Federal funds to provide effective control and accountability for all funds and assets received from the Department. The Departmental policies presented in this *Handbook* are interpretations of basic management practices that meet the requirements of CFR 45, Part 74. The Privacy Act of 1974 does not apply to grants and cooperative agreements.

EXHIBIT XII-A: SOLICITATION CERTIFICATION

Introduction: This form is an example for the Project Officer to use in certifying that the Statement of Work in a Request for Proposal complies with the security requirements of the Departmental AISSP. The Project Officer should complete all parts of this example form which are in parentheses.

To: (Identify the Contracting Officer)

Subject: Certification of Adequacy of Automated Information System (AIS) Security Requirements for (Identify acquisition)

I certify that the referenced Request for Proposal for the acquisition of (briefly describe goods or services to be acquired) specifies appropriate security requirements necessary to adequately protect the Government's interests in compliance with all Federal, DHHS, and OPDIV/Agency AIS security requirements as prescribed by OMB Circular A-130, Appendix III, "Security of Federal Automated Information Systems," and the *DHHS Automated Information Systems Security Program (AISSP) Handbook.* The security requirements are set forth in such a manner that all prospective contractors can readily understand what is required.

_____
Project Officer Signature

_____
Title

_____
Organization Information Systems
Security Officer Signature

EXHIBIT XII-B: PRE-AWARD CERTIFICATION

Introduction: This form is an example for the Project Officer to use in certifying that a proposal received in response to a Request for Proposal complies with the security requirements of the Departmental Automated Information Systems Security Program (AISSP). The Project Officer should complete all parts of this example form which are in parentheses.

To: (Identify the Contracting Officer)

Reference: (Identify the acquisition action and/or contracting effort)

I certify that the proposal from (identify the offeror), dated (indicate the date of the proposal), specifies appropriate security requirements necessary to comply with Office of Management and Budget (OMB) Circular A-130, Appendix III, "Security of Federal Automated Information Systems," and the *DHHS AISSP Handbook.*

_____
Project Officer Signature

_____
Title

_____
Organization Information Systems
Security Officer Signature

EXHIBIT XII-C: SECURITY POLICY STATEMENT FOR INCLUSION IN AUTOMATED INFORMATION SYSTEMS CONTRACTS

Introduction: This statement is an example for the Contracting Officer to include in all contracts which involve the development of an automated information system or the use of automated information system resources. The Contracting Officer should complete all parts of this example statement called for by the phrase "indicate. . .".

By accepting this contract, the contractor providing application systems or automated information system (AIS) resources to any component of the Department of Health and Human Services (DHHS) agrees to comply with the applicable AIS security policy as outlined in the Statement of Work. The contractor shall include this requirement in any subcontract awarded under this prime contract. Failure to comply with said requirements shall constitute cause for termination.

A written agreement between (indicate the DHHS component) and any contractor shall be entered into before data and information otherwise exempt from public disclosure may be disclosed to the contractor. (Disclosure statement attached.) The contractor shall agree to establish and follow security precautions considered by (indicate the DHHS component) to be necessary to ensure proper and confidential handling of data and information. This information is more specifically addressed in the *DHHS Automated Information Systems Security Program (AISSP) Handbook.*

Contractor employees in AIS-related positions must comply with the criteria for assigning position sensitivity designations in the *Federal Personnel Manual (FPM)* Section 732, "Personnel Security," dated January 6, 1984. These positions will be determined by the (indicate the DHHS component) Information Systems Security Officer and the (indicate the DHHS component) Project Officer.

Contractor employees assigned to the project in a Level 4C or 3C position must have a current completed/approved full field investigation. Contractor employees assigned to a Level 2C position require either a limited background investigation or a medium background investigation. A Level 1C position must have been processed and been approved by a National Agency Check and Inquiry (NACI) Investigation plus a Credit Check, or have been previously processed and approved by another approved agency or organization under appropriate authority for processing investigations.

Verification of these clearances, e.g., duplicate copies of processed forms verifying processing under Section 3(a) of Executive Order 10450, must be submitted to:

(Indicate the appropriate DHHS agency)
(office for verification)

prior to award of contract.

EXHIBIT XII-D: COMMITMENT TO PROTECT PRIVILEGED INFORMATION CONTRACTOR AGREEMENT

Introduction: This statement is an example for the Contracting Officer to include in the Statement of Work of a Request for Proposal which involves the development of an automated information system or the use of automated information system resources. The statement is to be completed by all contractor employees who would be involved in the performance of contract work.

Access to privileged information from the files of the (indicate the DHHS component) is required in the performance of my official duties, under contract number (indicate the contract number) between (indicate the DHHS component) and my employer, (indicate your company name). I, (indicate your name), on this ( ) day of 19( ), hereby agree that I shall not release, publish, or disclose such information to unauthorized personnel and I shall protect such information in accordance with the provisions of 18 U.S.C. 641, 18 U.S.C. 1905, Public Law 96-511, and other pertinent laws and regulations governing the confidentiality of privileged information.

I understand the provisions of 18 U.S.C. 641, 18 U.S.C. 2071, and Public Law 96-511 and that I am subject to criminal penalties prescribed by law for any violations thereof.

Signed: _____

Date: _____

Witnessed by: _____

Date: _____

Copies are retained by:
(Indicate the DHHS component)
(Indicate your company name)
(Indicate your name)

APPENDICES

OVERVIEW

Appendix A: References lists the general references used in developing the *AISSP Handbook*. The references listed are not exhaustive, but they are extremely useful. References have not been used which deal with specific agencies or information categories. Organization managers should seek counsel on specific laws and other issuances which bear on their organizational missions or deal with information they collect, administer, or process.

Appendix B: Control Requirements presents a composite set of 55 control requirements which constitute the core of the Departmental AISSP. The control requirements were initially derived from seven principal control directives and then used to establish the minimum security safeguards of the Departmental AISSP. (See Exhibit III-B: Matrix of Minimum Security Safeguards.)

Appendix C: Control Requirements Cross-Referenced to Major Control Directives presents the seven principal control directives used to establish the Departmental AISSP and cross-references the directives to the 55 control requirements which constitute the core of the Departmental AISSP.

Appendix D: Definitions defines common terms used in the *AISSP Handbook*.

Appendix E: Acronyms defines all acronyms used in the *AISSP Handbook*.

A. PUBLIC POLICY AND LAW

1. Privacy Act of 1974, December 31, 1974, P.L. 93-579, 5 U.S.C. 552a

2. Paperwork Reduction Act of 1980, December 11, 1980, P.L. 96-511, 44 U.S.C. 3501-3520, as amended in the Paperwork Reauthorization Act.

3. Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, October 12, 1984, 18 U.S.C. 1030

4. Computer Security Act of 1987, January 8, 1988, P.L. 100-235

5. Computer Crime Act of 1984

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

7. Public Information Agency Rules, Opinions, Records, and Proceedings (Freedom of Information Act), 5 U.S.C. 552 (1967)

8. Records Maintained on Individuals (Privacy Act of 1974), 5 U.S.C. 552a (1974)

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

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

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

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

13. Public Health Service Act

14. Food, Drug, and Cosmetic Act

B. OFFICE OF MANAGEMENT AND BUDGET

1. OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Systems, December 12, 1985

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

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

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

4A. OMB Privacy Act Guidelines published in the Federal Register (FR) 40, 28934-28978, July 9, 1975

4B. OMB Supplementary Privacy Act Guidance, FR 40, 56741-56743, December 4, 1975

4C. OMB Memorandum "Application of Subsection M of the Privacy Act," November 30, 1979

4D. OMB Revised Supplemental Guidance for Conducting Computer Matching Programs, FR 47, 21656-21658, May 19, 1982

C. GENERAL SERVICES ADMINISTRATION

1. Federal Information Resources Management Regulation (FIRMR) Part 202-2, Definitions, and Part 201-6, Protection of Personal Privacy

2. FIRMR Part 201-7, Security of Information Resource Systems

3. FIRMR Part 201-8, Implementation and Use of Federal Standards

4. FIRMR Part 201-30, Management of ADP Resources

5. FIRMR Part 201-32, Contracting for ADP Resources

6. FIRMR Part 201-38, Management of Telecommunication Resources

7. FIRMR Part 201-40, Contracting for Telecommunications Resources

8. 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

D. OFFICE OF PERSONNEL MANAGEMENT

1. Federal Personnel Manual (FPM) Chapter 732, Personnel Security

2. 5 Code of Federal Regulations (CFR) Part 930, Training Requirements for the Computer Security Act

E. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

1. Federal Information Processing Standards Publication (FIPS PUB) 31, Guidelines for Automated Data Processing Physical Security and Risk Management

2. FIPS PUB 39, Glossary of Computer Systems Security

3. FIPS PUB 41, Computer Security Guidelines for Implementing the Privacy Act of 1974

4. FIPS PUB 46, Data Encryption Standard (DES)

5. FIPS PUB 48, Guidelines on Evaluation Techniques for Automated Personnel Identification

6. FIPS PUB 65, Guideline for Automated Data Processing Risk Analysis

7. FIPS PUB 73, Guidelines for Security of Computer Applications

8. FIPS PUB 81, DES Modes of Operation

9. FIPS PUB 83, Guideline on User Authentication Techniques for Computer Network Access Control

10. FIPS PUB 87, Guidelines for ADP Contingency Planning

11. FIPS PUB 88, Guideline for Integrity Assurance and Control in Database Administration

12. FIPS PUB 102, Guideline for Computer Security Certification and Accreditation

13. FIPS PUB 112, Password Usage

14. FIPS PUB 113, Computer Data Authentication

15. Special Publication 500-120, Security of Personal Computer Systems: A Management Guide

16. Special Publication 500-137, Security for Dial-Up Lines
17. NIST Special Publication 500-166, Computer Viruses and Related Threats: A Management Guide, August 1989.

18. NIST Special Publication 500-169, Executive Guide to the Protection of Information Resources, October 1989.

19. NIST Special Publication 500-170, Management Guide to the Protection of Information, October 1989.

20. NIST Special Publication 500-171, Computer User's Guide to the Protection of Information Resources, October 1989.

21. NIST Special Publication 500-172, Computer Security Training Guidelines, November 1989.

22. NIST Special Publication 500-173, Guide to Data Administration, October 1989.

23. NIST Special Publication 500-174, Guide to Selecting Automated Risk Analysis Tools, October 1989.

F. DEPARTMENT OF DEFENSE

1. DOD 5200.28 STD, Trusted Computer Systems Evaluation Criteria, December 1985

2. CSC-STD-003-85, Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments, June 25, 1985

G. NATIONAL TELECOMMUNICATION AND INFORMATION SYSTEMS SECURITY

1. 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. DEPARTMENT OF HEALTH AND HUMAN SERVICES

1. DHHS General Administration Manual Chapter 7, Physical Security Policy, and Part 45, Privacy Act Guidance

2. DHHS Information Resources Management Manual, Part 6, AIS Security Training and Orientation Program Guide, February 1991.

3. DHHS Internal Controls Manual, Chapters 1 through 5, December 1984

4. DHHS Instruction 731-1, Personnel Manual, Personnel Security/Suitability - Policy and Guidance, August 4, 1988

5. DHHS Records Management Manual Revised Draft Chapters 10 through 80, April 1988

6. DHHS Transmittal 85.01, Information Security Manual, Chapters 1 through 13 on the safeguarding, disposal, and use of documents containing National Security (Classified) Information, November 1, 1985

7. 45 Code of Federal Regulations (CFR), DHHS Freedom of Information Act Regulations

8. 45 Code of Federal Regulations (CFR) Subpart 5B, DHHS Privacy Act Regulations

Item No.	Requirements

I. APPLICATION CONTROLS (1-7)

1 **Transactions are authorized.** Management must authorize information entered into automated information systems.

2 **Transactions are valid.** Automated information systems must process only data that represent legitimate events.

3 **Information is complete.** Only valid data may be processed by an automated information system.

4 **Information is accurate.** Data must be free from error during all phases of processing, within defined levels of tolerance.

5 **Information is timely.** Data must reflect the correct cycle, version, or period for the processing being performed. Financial management data must be recorded as soon as practical after the occurrence of the event, and relevant preliminary data must be made available to managers promptly after the end of the reporting period.

6 **System and data are secure.** Data files, computer programs, and equipment must be secure from unauthorized changes, accidental changes, unauthorized disclosure and use, and physical destruction. Detective and corrective controls may also apply, depending on the sensitivity level designation of system data.

7 **System is auditable.** An information trail must exist that establishes individual accountability for transactions and permits an analysis of breakdowns and other anomalies in the system.

II. GENERAL CONTROLS (8-33)

8 **System controls exist.** The controls system for each automated information system must ensure that appropriate safeguards are incorporated into the system, tested before implementation, and tested periodically after implementation.

9 **Five-year system plan developed.** Each Agency must develop a plan including specific milestones with obligation and outlay estimates for every automated information system in the Agency. This includes both current automated information systems and those under development.

Item No.	Requirements
10	**Contingency plan/disaster recovery plan exists.** Agencies must develop, maintain, and test disaster recovery and continuity of operations plans for their data center(s) to provide reasonable continuity of data processing support if normal operations are prevented.
11	**Vulnerability assessment conducted.** Agencies must review the susceptibility of their programs or functions to waste, loss, unauthorized use, or misappropriation. This includes vulnerability assessments and equivalent reviews, such as audits.
12	**Cost/benefit analysis exists.** Agencies must determine and compare the benefits of proposed systems or controls against the cost of developing and operating the systems or controls. Only those proposals where the expected benefits exceed the estimated costs by 10 percent should be considered for development, unless otherwise specifically required by statute.
13	**Reasonable assurance applied.** Reasonable assurance equates to a satisfactory level of confidence, based on management's judgement of the cost/benefits of controls versus recognized risks. It is recognized that it is not cost-effective to attain 100 percent assurance. Each Agency must provide reasonable assurance.
14	**Control objectives defined.** Agencies must establish goals to address known vulnerabilities or promote reliability or security of automated information systems.
15	**Control techniques selected.** Agencies must develop methods to satisfy control requirements by preventing, detecting, and/or correcting undesired events.
16	**Adequacy of security requirements determined.** Agencies must ensure that appropriate technical, administrative, physical, and personnel security requirements are included in specifications for the acquisition or operation of automated information system facilities, equipment, or software.
17	**Security specifications exist.** Internal control and security requirements must be stated as design specifications and approved by management before development (programming) of application systems.
18	**Adequacy of security specifications determined.** Agencies must present proof to management that design specifications satisfy control requirements to authorize computer program development and/or modification (programming).

Item No.	Requirements

19 **System design approved.** Before development (programming) of an automated information system is authorized, management must be assured that the system design satisfies the user's requirements and incorporates the control requirements. The design review must be documented and be available for examination.

20 **Controls documented.** Internal control systems, including all transactions and significant events, must be clearly documented and readily available for examination.

21 **System documentation exists.** Documentation must reflect the current state of an automated information system as it is being operated. The documentation must be sufficient to ensure effective operation by users and system maintenance by programmers.

22 **System contingency plan exists.** Plans must be developed, documented, and tested to assure that the users of automated information systems can continue to perform essential functions in the event that processing capability is interrupted. The plan must also be consistent with the Agency-wide disaster recovery plan.

23 **Controls tested.** Before a new or modified automated information system is placed into production status, its controls must be tested to prove that they operate as intended. The test results must be documented and sent to management for approval prior to implementation of the system.

24 **System test conducted.** Before implementation of an automated information system is authorized, evidence that the system operates as intended must be presented to management. This evidence must also include the results of controls testing. The test results must be documented and available for examination.

25 **Test results documented.** Documentation must demonstrate that the control and functionality requirements of automated information systems operate as intended.

26 **System certified prior to implementation.** Before an automated information system can be implemented, an Agency official must certify that the system meets all applicable Federal policies, regulations, and standards, and that test results demonstrate that installed controls are adequate for the system.

27 **Controls review performed.** Periodically, each automated information system must be tested to determine if its controls still function as intended. The results of these tests must be documented and available for examination.

Item No.	Requirements

28 **Periodic reviews and recertifications are conducted.** At least once every 3 years, Agencies must review their automated information systems and recertify the adequacy of their safeguards. The recertifications must be documented and available for review.

29 **Periodic risk assessments are conducted.** Agencies must conduct periodic risk assessments at their automated information facilities to provide a measure of the relative vulnerabilities and threats to the facilities so that security resources can be effectively distributed to minimize potential loss.

30 **Corrective action taken; audit findings resolved promptly.** Managers must promptly evaluate audit findings and recommendations, determine proper corrective actions, and complete those actions.

31 **Annual report on internal controls prepared.** Each Agency must annually determine if its systems of internal controls are in compliance with the Comptroller General's standards.

32 **Annual report on accounting systems prepared.** Each Agency must annually determine if its accounting systems are in compliance with the Comptroller General's standards.

33 **Annual reports sent to President.** The head of each Agency must sign both annual reports and transmit them to both the President and Congress.

III. ADMINISTRATIVE CONTROLS (34-45)

34 **Organizational responsibility is affixed.** Responsibilities must be assigned for planning, directing, and controlling the controls evaluations process for the organization. The programs and functions conducted in each organizational component must also be specified.

35 **Separation of duties exists.** Key duties and responsibilities in authorizing, processing, recording, and reviewing transactions must be separated among individuals.

36 **Supervision is provided.** Qualified and continuous supervision must be provided to ensure that control requirements are met.

37 **Supportive attitudes exist.** Managers and employees should maintain and demonstrate a positive and supportive attitude toward controls at all times.

Item No.	Requirements

38 **Personnel are competent.** Managers and employees should have personal and professional integrity and maintain a level of competence that allows them to accomplish their assigned duties, as well as understanding the importance of developing and implementing good controls.

39 **Security training program exists.** Agencies must establish a security awareness and training program so that Agency and contractor personnel involved with automated information systems are aware of their security responsibilities and know how to fulfill them.

40 **Written policies and procedures exist.** Each Agency must establish administrative procedures to enforce the intended functioning of controls, and provisions that performance appraisals reflect execution of control-related responsibilities.

41 **Personnel security policies exist.** Each Agency must establish and manage personnel security procedures, including requirements for screening Agency and contractor personnel involved in the design, development, operation, maintenance, or use of automated information systems. The level of screening depends on the sensitivity level designation of system data.

42 **Individual responsibilities are affixed.** Assignments of responsibility must be made for internal controls, accounting systems, and data center security on an Agency-wide and individual system/center basis.

43 **Custody/accountability assigned.** Each official whose function is supported by an automated information system is responsible and accountable for the products of the system.

44 **Record retention procedures exist.** Each Agency must establish procedures for the retention, archiving, and destruction of data files.

45 **Release of information is provided for.** Each Agency must have procedures in place so that information can be extracted from systems to meet requests made under the Privacy Act and the Freedom of Information Act.

IV. REQUIRED SYSTEM FUNCTIONS (46-55)

46 **System is efficient.** The benefits of an automated information system must exceed the costs to develop or operate the system.

Item No.	Requirements
47	**System operation is economical.** Even if a proposed automated information system is cost beneficial, the Agency must determine if the system is affordable to develop and continues to be affordable to operate. Uneconomical systems must be identified and phased out.
48	**System is effective.** Periodically, each automated information system must be reviewed to determine if the system still meets organizational needs.
49	**System supports management.** Data must be recorded and reported in a manner to facilitate the fulfillment of responsibilities of both program and administrative managers.
50	**System supports budget.** Financial management data must be recorded, stored, and reported to facilitate budget preparation, analysis, and execution.
51	**Comparability/consistency provided for.** Financial management data must be recorded and reported in the same manner throughout an Agency, using uniform definitions that are synchronized with budgeting for each reporting period.
52	**System is useful/relevant.** Data capture and reports must be tailored to specific user needs, and, if usage does not justify costs, the data or reports must be terminated.
53	**System provides full disclosure.** Data must be recorded and reported in a manner to provide users of the data with complete information about the subject of the report per OMB, Treasury, and Privacy Act standards.
54	**Individual access allowed.** Automated information systems must be able to extract any data contained in a data base about an individual in response to a request by that individual or his/her representative when required by the Privacy Act.
55	**Network compatibility exists.** All new automated information systems developed or acquired must be compatible with any existing system that will be linked to the new system.

ITEM NO.	REQUIREMENTS	OMB A-123	OMB 1C	OMB A-127	OMB A-130	GAO TITLE II	FMFIA	PRIVACY ACT
I.	**APPLICATION CONTROLS (1-7)**							
1	Transactions are authorized	X	X		X	X		X
2	Transactions are valid	X	X		X	X		
3	Information is complete	X	X	X		X	X	X
4	Information is accurate	X	X	X	X	X	X	X
5	Information is timely	X	X	X		X	X	X
6	System and data are secure				X		X	X
7	System is auditable			X		X		
II.	**GENERAL CONTROLS (8-33)**							
8	System controls exist				X	X		
9	Five-year system plan developed			X	X	X		
10	Contingency plan/disaster recovery plan exists				X	X		
11	Vulnerability assessment conducted	X	X			X		
12	Cost/benefit analysis exists					X		X
13	Reasonable assurance applied	X	X	X	X	X	X	
14	Control objectives defined	X	X			X		
15	Control techniques selected	X	X			X		
16	Adequacy of security requirements determined				X			X
17	Security specifications exist				X	X		
18	Adequacy of security specifications determined				X			

ITEM NO.	REQUIREMENTS	OMB A-123	OMB 1C	OMB A-127	OMB A-130	GAO TITLE II	FMFIA	PRIVACY ACT
19	System design approved				X	X		
20	Controls documented	X	X			X		
21	System documentation exists					X		
22	System contingency plan exists				X	X		
23	Controls tested				X	X		
24	System test conducted					X		
25	Test results documented				X	X		
26	System certified prior to implementation				X			
27	Controls review performed	X	X	X		X	X	
28	Periodic reviews and recertifications are conducted			X	X	X		X
29	Periodic risk assessments are conducted				X	X		
30	Corrective action taken; audit findings resolved promptly	X	X			X		
31	Annual report on internal controls prepared		X	X		X		
32	Annual report on accounting systems prepared					X	X	
33	Annual reports sent to President	X	X		X	X	X	

ITEM NO.	REQUIREMENTS	OMB A-123	OMB 1C	OMB A-127	OMB A-130	GAO TITLE II	FMFIA	PRIVACY ACT
III.	**ADMINISTRATIVE CONTROLS (34-45)**							
34	Organizational responsibility is affixed		X					X
35	Separation of duties exists	X	X			X		
36	Supervision is provided	X	X			X		
37	Supportive attitudes exist	X	X			X		
38	Personnel are competent	X	X			X		
39	Security training program exists				X			
40	Written policies and procedures exist	X	X	X				X
41	Personnel security policies exist				X			
42	Individual responsibilities are affixed	X	X	X	X	X		
43	Custody/accountability assigned	X	X		X	X	X	
44	Record retention procedures exist							X
45	Release of information is provided for							X

ITEM NO.	REQUIREMENTS	OMB A-123	OMB 1C	OMB A-127	OMB A-130	GAO TITLE II	FMFIA	PRIVACY ACT
IV.	**REQUIRED SYSTEM FUNCTIONS (46-55)**							
46	System is efficient			X		X		
47	System operation is economical			X		X		
48	System is effective				X	X		
49	System supports management			X				
50	System supports budget			X		X		
51	Comparability/consistency provided for			X		X		
52	System is useful/relevant			X	X	X		X
53	System provides full disclosure			X		X		X
54	Individual access allowed				X		X	X
55	Network compatibility exists				X			

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.[1]

AGENCY Agency means any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government, or any independent regulatory agency. Within the Executive Office of the President, the term includes only the Office of Management and Budget and the Office of Administration.[1]

APPLICATION SYSTEM An application system is a software package which processes, transmits, or disseminates information according to established internal procedures. An application system is run on an automated information system facility. A word processor usually runs only one application system. A mainframe computer may run thousands of application systems.

AUTOMATED INFORMATION SYSTEM (AIS) An AIS is the organized collection, processing, transmission, and dissemination of automated information in accordance with defined procedures.[1]

AUTOMATED INFORMATION SYSTEM (AIS, ADP, OR COMPUTER) ASSETS AIS, ADP, or computer assets are the personnel and/or property associated with or accessible by an AIS, office automation, or telecommunications, including information, data, programs, equipment, facilities, supplies, services, software, personal computers, processing time, and money.

AUTOMATED INFORMATION SYSTEM (AIS) FACILITY An AIS facility is an organizationally defined set of personnel, hardware, software, and physical facilities, a primary function of which is the operation of an automated information system(s) and an application system(s). AIS facilities range from large centralized computer centers to individual stand-alone microprocessors such as personal computers and word processors.

AUTOMATED INFORMATION SYSTEM (AIS, ADP, OR COMPUTER) SECURITY AIS, ADP, or computer security refers to the combination of physical, administrative, and technical measures applied to protect AIS assets from loss, destruction, misuse, alteration, or unauthorized disclosure or access.

COMPUTER SYSTEM Any equipment or interconnected system or subsystems of equipment used in automatic acquisition storage manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information; and includes 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.[2]

CONTINGENCY PLANNING Contingency planning refers to the develop-ment, testing, and maintenance of plans for emergency response, backup operations, and disaster recovery at an AIS facility where data and information are processed.

DATA FILE A data file is a compilation of Government information which shares specified descriptive characteristics. A data file is created, collected, processed, transmitted, disseminated, used, stored, and disposed of by application systems. The protection of data files is the cornerstone of the entire Departmental AISSP.

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, intra-agency sharing of information, or responding to public requests for access to information.

FEDERAL COMPUTER SYSTEM A Federal computer system is a computer 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 proc-essing (ADP) equipment as that term is defined in section 111(a)(2) of the Federal Property and Administrative Services Act of 1949.[2]

GOVERNMENT INFORMATION Government information is any information that is created, collected, processed, transmitted, disseminated, used, stored, or disposed of by the Federal Government.[1]

GOVERNMENT PUBLICATION A Government publication is informational matter which is published as an individual document at Government expense, or as required by law.[1]

INFORMATION Information is any communication or reception of knowledge, such as facts, data, and opinions, including numerical, graphic, or narrative forms, whether oral or maintained in any other medium, including computerized data bases, paper, microform, or magnetic tape.[1]

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.[1]

INFORMATION SYSTEMS SECURITY (INFOSEC) An INFOSEC is a composite of factors necessary to protect Federal Information Processing systems and the information they process to prevent exploitation through interception, unauthorized electronic access, or related technical intelligence threats, and to ensure authenticity. This protection results from the application of security measures; including cryptosecurity, transmission security, emission security, and computer security; to systems that generate, store, process transfer or communicate information of use to an adversary, and also includes the physical protection of sensitive material and sensitive technical security.

INFORMATION TECHNOLOGY UTILITY (ITU) An ITU is an organizationally defined set of personnel, hardware, software, and physical facilities, a primary function of which is to coordinate the operation of geographically dispersed automated information systems and automated information system facilities. ITUs range in size from wide area networks covering widely dispersed geographical areas to local area networks covering a single office.

PERSONNEL SECURITY Personnel security refers to a program that determines the sensitivity of positions and screens individuals who participate in the design, operation, or maintenance of automated information systems or who have access to such systems.

PHYSICAL SECURITY Physical security refers to the combination of devices that bar, detect, monitor, restrict, or otherwise control access to sensitive areas. Physical security also refers to the measures to protect a facility that houses AIS assets and its contents from damage by accident, malicious intent, fire, loss of utilities, environmental hazards, and unauthorized access.

RESOURCES Resources refers to all agency AIS assets.

RISK ANALYSIS A risk analysis is an assessment of the threats to and the vulnerability of a system or an installation. The analysis may vary from an informal review of microcomputer installation to a formal, fully quantified risk analysis of a large scale computer center.

RISK MANAGEMENT Risk management is a process for minimizing losses through the periodic assessment of potential hazards and the systematic application of corrective measures.

SECURITY SPECIFICATION A security specification is a detailed description of the safeguards required to protect a sensitive application (or any AIS asset).[1]

SENSITIVE APPLICATION A sensitive application is an application system which requires protection because it processes sensitive information or because of the risk and high magnitude of loss or harm that could result from its improper operation, deliberate manipulation (or delivery interruption) of the application.[2]

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.[1]

SENSITIVE INFORMATION Sensitive information is any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.[2]

SIGNIFICANT CHANGE A significant change is a physical, adminis-trative, or technical modification that alters the degree of protection required. Examples are adding a local area network, changing from batch to on-line processing, adding dial-up capa-bility, increasing the equipment capacity of the installation, etc.

TELECOMMUNICATIONS SYSTEMS Telecommunications systems are single or integrated combinations of equipment, services, or networks that transmit, emit, or receive information by wire, radio, optical, or other electromagnetic means.

USER A user is any organizational or programmatic entity that utilizes or receives service from an automated information system (AIS) 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.[1]

---

1 OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Systems, December 12, 1985.

2 Computer Security Act of 1987, January 8, 1988, P.L. 100-235.

ADP	Automated Data Processing
AIS	Automated Information System
AIS-STOP	Automated Information Systems Security Training and Orientation Program
AISI	Automated Information Systems Inventory
AISSP	Automated Information Systems Security Program
ASPER	Assistant Secretary for Personnel Administration
ASMB	Assistant Secretary for Management and Budget
CFR	Code of Federal Regulations
COM	Computer Output Microfilm
CPU	Central Processing Unit
CRT	Cathode Ray Tube
CSSP	Computer Systems Security Plan
DAS/ASM	Deputy Assistant Secretary for Administrative and Management Services
DAS/F	Deputy Assistant Secretary for Finance
DAS/IRM	Deputy Assistant Secretary for Information Resources Management
DAS/PAL	Deputy Assistant Secretary for Procurement, Assistance and Logistics
DAS/MAS	Deputy Assistant Secretary for Management Analysis and Systems
DODCI	Department of Defense Computer Institute
FIPS	Federal Information Processing Standards
FIRMR	Federal Information Resources Management Regulations
FPM	Federal Personnel Manual
FPMR	Federal Procurement Management Regulation
FR	Federal Register
GSA	General Services Administration
DHHS	Department of Health and Human Services
ICR	Internal Controls Review
IR	Information Resources
IRM	Information Resources Management
IRSP	Information Resources Security Program
IS	Information System
ISI	Information Systems Inventory
ISSO	Information Systems Security Officer
ITS	Information Technology Systems
ITU	Information Technology Utility

NACI	National Agency Check and Inquiry
NCSC	National Computer Security Center
NFPA	National Fire Protection Association
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSDD	National Security Decision Directive
OA	Office Automation
OCR	Optical Character Recognition
ODPC	Off-site Data Processing Center
OFMS	Office of Facilities and Management Services
OMB	Office of Management and Budget
OPDIV	Operating Division
OPF	Official Personnel Folder
OPM	Office of Personnel Management
OS	Office of the Secretary
PAO/C	Privacy Act Officer/Coordinator
PC	Personal Computer
PISG	Personnel Information and Security Group
PUBS	Publications
RD	Regional Director
RFC	Request for Contract
RFR	Request for Proposal
RJE	Remote Job Entry
RO	Regional Office
RSR	Recertification Security Review
SOW	Statement of Work
SPSO	Servicing Personnel Security Officer
SSA	Social Security Administration
STAFFDIV	Staff Division
TDG	Training and Development Group
WP	Word Processor

NIST-114A
(REV. 3-90)

U.S. DEPARTMENT OF COMMERCE
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

BIBLIOGRAPHIC DATA SHEET

1. PUBLICATION OR REPORT NUMBER
NISTIR 4636

2. PERFORMING ORGANIZATION REPORT NUMBER

3. PUBLICATION DATE
July 1991

4. TITLE AND SUBTITLE
U.S. Department of Health and Human Services' (HHS)
Automated INformation Systems Security Program Handbook

5. AUTHOR(S)
Edward Roback, NIST Coordinator

6. PERFORMING ORGANIZATION (IF JOINT OR OTHER THAN NIST, SEE INSTRUCTIONS)
U.S. DEPARTMENT OF COMMERCE
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
GAITHERSBURG, MD 20899

7. CONTRACT/GRANT NUMBER

8. TYPE OF REPORT AND PERIOD COVERED
NISTIR

9. SPONSORING ORGANIZATION NAME AND COMPLETE ADDRESS (STREET, CITY, STATE, ZIP)
Reprinted by permission of Department of Health & Human Services, Washington, DC

10. SUPPLEMENTARY NOTES

11. ABSTRACT (A 200-WORD OR LESS FACTUAL SUMMARY OF MOST SIGNIFICANT INFORMATION. IF DOCUMENT INCLUDES A SIGNIFICANT BIBLIOGRAPHY OR LITERATURE SURVEY, MENTION IT HERE.)

This Interagency Report presents the U.S. Department of Health and Human Services' (HHS) Automated Information Systems Security Program Handbook which provides a comprehensive description of the program elements which comprise HHS's approach to computer security. Among the varied items included are: security policy and responsibilities, security level designators, security level requirements, security administration, risk management, contingency planning, personnel security, facility security, application systems and data security, personal computers, data communications, and acquisitions and contracts.

12. KEY WORDS (6 TO 12 ENTRIES; ALPHABETICAL ORDER; CAPITALIZE ONLY PROPER NAMES; AND SEPARATE KEY WORDS BY SEMICOLONS)
ADP security; automated information system security; certification; computer security; contingency planning; risk assessment; telecommunications security

13. AVAILABILITY

[X] UNLIMITED

[ ] FOR OFFICIAL DISTRIBUTION. DO NOT RELEASE TO NATIONAL TECHNICAL INFORMATION SERVICE (NTIS).

[ ] ORDER FROM SUPERINTENDENT OF DOCUMENTS, U.S. GOVERNMENT PRINTING OFFICE, WASHINGTON, DC 20402.

[X] ORDER FROM NATIONAL TECHNICAL INFORMATION SERVICE (NTIS), SPRINGFIELD, VA 22161.

14. NUMBER OF PRINTED PAGES
150

15. PRICE
A07

ELECTRONIC FORM