United States
Environmental Protection
Agency

Administration and
Resources Management
(PM-211D)

21M-1008
December 1989

EPA

Information Security Manual

PREFACE

Recently, information security has achieved a new and unfamiliar prominence. Information security issues have appeared on the covers of both "Time" and "Business Week" magazines. Congress has emphasized the importance of information security through its passage of the Computer Security Act of 1987.

What this newfound prominence seems to highlight is that we are now truly in the Age of Information. The explosion in personal computing is the latest step in creating this information society. As we have become more dependent on our information resources, so have we also become more concerned about what might happen if those resources were lost or misused.

At the Environmental Protection Agency (EPA), the Agency information security policy is contained in a formal policy statement. (The policy statement, issued in 1987, is reproduced here as Appendix A.) The policy statement recognizes that information is an Agency asset and that the EPA is highly dependent on its information resources to carry out program and administrative functions in a timely, efficient, and accountable manner.

The policy statement formally establishes a comprehensive, Agency-wide information security program and describes individual and organizational responsibilities under the program. Two procedural manuals which explain to EPA managers and staff how to comply with these responsibilities have now been developed.

This is one of the two manuals and it deals comprehensively with all types of information assets (paper records, mainframes and minicomputers, information systems, PCs, and word processors). The other manual deals exclusively with PC security. Because PC security affects the most employees and is a relatively new area of security vulnerability, it is important to handle it separately so that the PC procedures will be accessible and will not get lost in discussions of mainframe or software development security.

Each manual begins with similar introductory sections. Information security and information sensitivity are defined in terms of the three objectives of the EPA program, which are to maintain information availability, integrity, and confidentiality. The information security problem is then described in terms of threats to the objectives.

Printed on Recycled Paper

Each manual is structured to allow the reader, whether manager or staff member, to tailor it to his/her own particular security situation by completing one or two worksheets and by reading selected portions of the text. Specifically, each reader works through a sensitivity evaluation table to determine if he/she has sensitive information. If not, only minimal security controls need to be implemented. If the reader does have sensitive information, he/she uses a worksheet to identify why the information is sensitive and which of the three security objectives are relevant. The reader is then referred to later sections of the manual as appropriate. For example, there is a subsection on safeguards for maintaining the availability of critical PC applications and a subsection on safeguards for preserving the confidentiality of confidential paper records.

Because a common problem in information security is determining exactly who is responsible for what aspects of security, each manual devotes a chapter to information security roles and responsibilities. While the manuals are as user friendly as possible in explaining to readers how to fulfill those responsibilities, they are not painless. To ensure that information resources are adequately protected, they describe three different control processes. The processes establish a structure of security checks and balances by approaching security both from an equipment perspective and from an application or information system perspective.

TABLE OF CONTENTS

Section	Page
1. GENERAL INFORMATION	1-1
2. INFORMATION SECURITY ROLES AND RESPONSIBILITIES	2-1
3. MINIMAL SECURITY CONTROLS FOR MINICOMPUTER/MAINFRAME INSTALLATIONS, PCs, PC LANS, AND WORD PROCESSORS	3-1
4. DETERMINING THE NEED FOR ADDITIONAL CONTROLS	4-1
5. PERSONNEL SECURITY AND TRAINING	5-1
6. SECURITY FOR MINICOMPUTER AND MAINFRAME INSTALLATIONS	6-1
7. SECURITY FOR PERSONAL COMPUTERS AND PC LANs	7-1
8. SECURITY FOR WORD PROCESSORS	8-1
9. SECURITY FOR APPLICATION SYSTEM DEVELOPMENT, OPERATIONS AND MAINTENANCE	9-1
10. SECURITY FOR PAPER RECORDS	10-1
APPENDIX A: POLICY	A-1
APPENDIX B: APPLICATION RISK ANALYSIS AND APPLICATION CERTIFICATION	B-1
APPENDIX C: INSTALLATION RISK ANALYSIS	C-1
APPENDIX D: DISASTER RECOVERY AND CONTINUITY OF OPERATIONS PLANS	D-1

1. GENERAL INFORMATION

1.1 PURPOSE, SCOPE, AND APPLICABILITY

In accordance with the Agency's Information Security Policy, this manual establishes security procedures for safeguarding Agency information resources and provides overall guidance to EPA managers and staff in implementing those procedures. The security controls specified in this manual are designed to ensure that information resources are adequately protected and that EPA organizations and staff are in compliance with all requirements of the policy.

As used in this manual, information resource (or information asset) is a broad term. It includes automated information systems, computerized data bases, computer programs, collections of paper records, information on microfiche or microfilm, and computer installations.

Consistent with the Information Security Policy, this manual applies to all EPA organizations and their employees. It also applies to the personnel of agents (including contractors and grantees) of the EPA who are involved in designing, developing, operating, or maintaining Agency information and information systems.

The specific purposes of this manual are as follows:

- To save organizations money by ensuring that only focused, cost-effective security safeguards (or controls) are implemented
- To protect organizations and individuals from the embarrassment of an unauthorized disclosure or from the disruption that would result if critical information were destroyed
- To help organizations meet internal control review requirements by providing them with a sound basis for assuring that automated information systems are adequately protected
- To assist staff in developing the system documentation required by the "EPA System Design and Development Guidance"
- To enable organizations to successfully undergo any security audits that may be conducted by the Office of the Inspector General.

1.2 INTRODUCTION TO THE EPA INFORMATION SECURITY PROGRAM

Through the Information Security Policy, the EPA has established a comprehensive, Agency-wide information security program to adequately safeguard the Agency's information resources. (The policy, which is Chapter 8 of the EPA's "Information Resources Management Policy Manual," is reproduced here as Appendix A.) The concept of adequacy means that security controls should be neither overapplied nor underapplied. Overapplication wastes financial and ADP resources, and underapplication exposes the information to various security threats.

The policy categorizes information and applications (or systems) as either sensitive or not sensitive. Sensitive information means information that requires protection due to the loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information. Examples of sensitive information include Confidential Business Information (CBI), Privacy Act Information, and data critical to the performance of primary Agency missions. A sensitive application is an application that processes sensitive information or an application that requires protection because of the loss or harm that could result from the improper operation or deliberate manipulation of the application itself.

In short, information security involves the precautions taken to protect sensitive information resources from potential loss and misuse. The three major objectives of the EPA program, as illustrated in Exhibit 1-1, are to maintain:

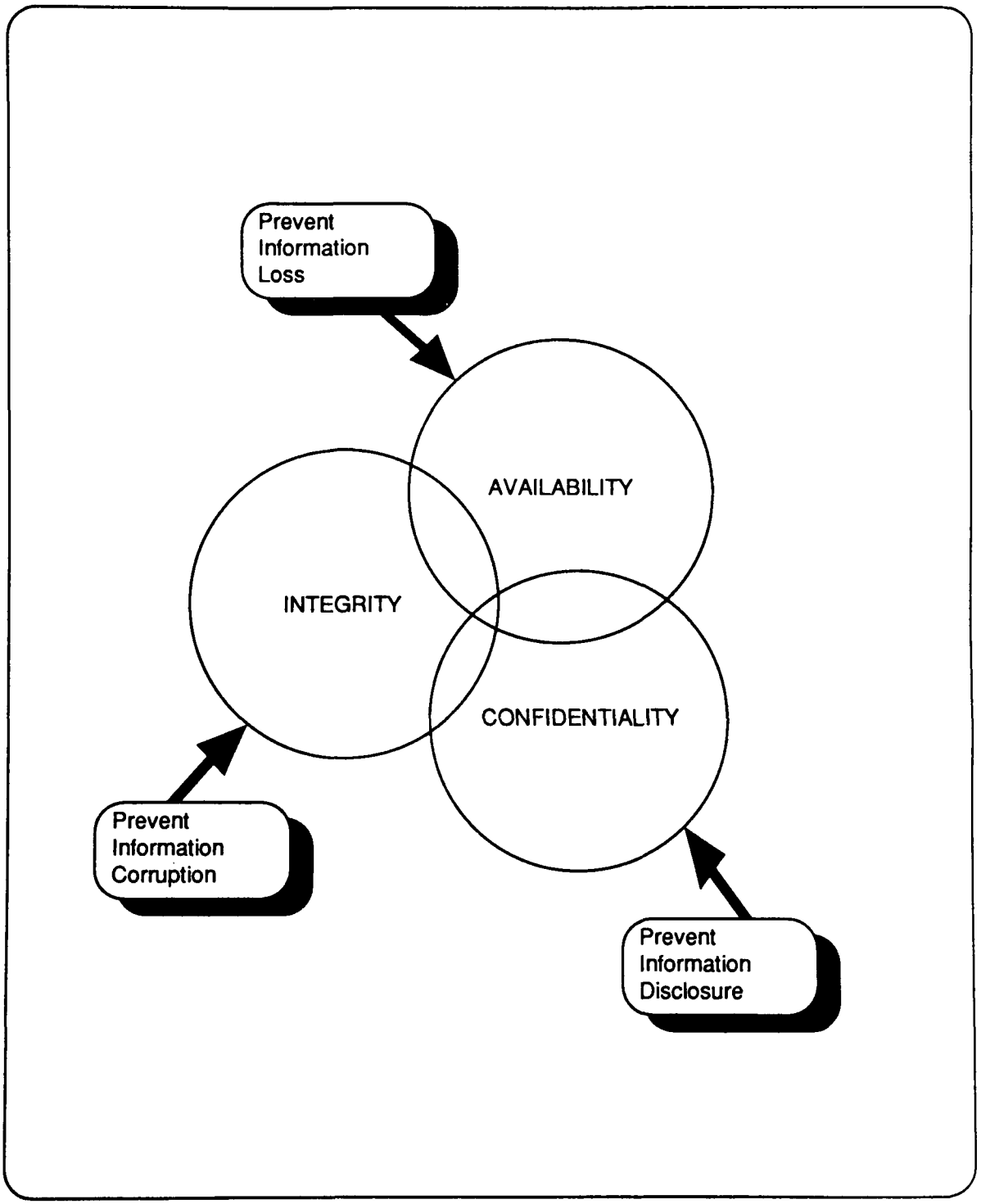
- Information Availability
- Information Integrity
- Information Confidentiality

The availability objective is associated with information where the loss of the information would cause serious problems, either because it would be costly to replace the information or because it would be difficult to function without the information. Thus, availability involves both the dollar value and the time value (or criticality) of the information. An example of an Agency information system or application where availability is important is the Resource Conservation and Recovery Information System (RCRIS).

The integrity objective is associated with information or applications where accuracy

EXHIBIT 1-1

INFORMATION SECURITY OBJECTIVES



and reliability are of particular concern. In short, integrity is concerned with protecting information from corruption. An example of an Agency information system where integrity is important is the Integrated Financial Management System (IFMS).

The confidentiality objective is concerned with information where disclosure would be undesirable or unlawful. Examples of information of this type include Toxic Substances Control Act (TSCA) CBI or personnel files.

As Exhibit 1-1 indicates, a particular application could involve only one objective or could involve some combination of objectives. For example, a data base could contain information critical to a primary Agency mission and yet contain no confidential information. In other words, while the availability objective is key, confidentiality is not a factor and the information in the data base could be widely disseminated without any damage resulting from disclosure. On the other hand, another data base could be both critical and confidential.

1.3 THE INFORMATION SECURITY PROBLEM

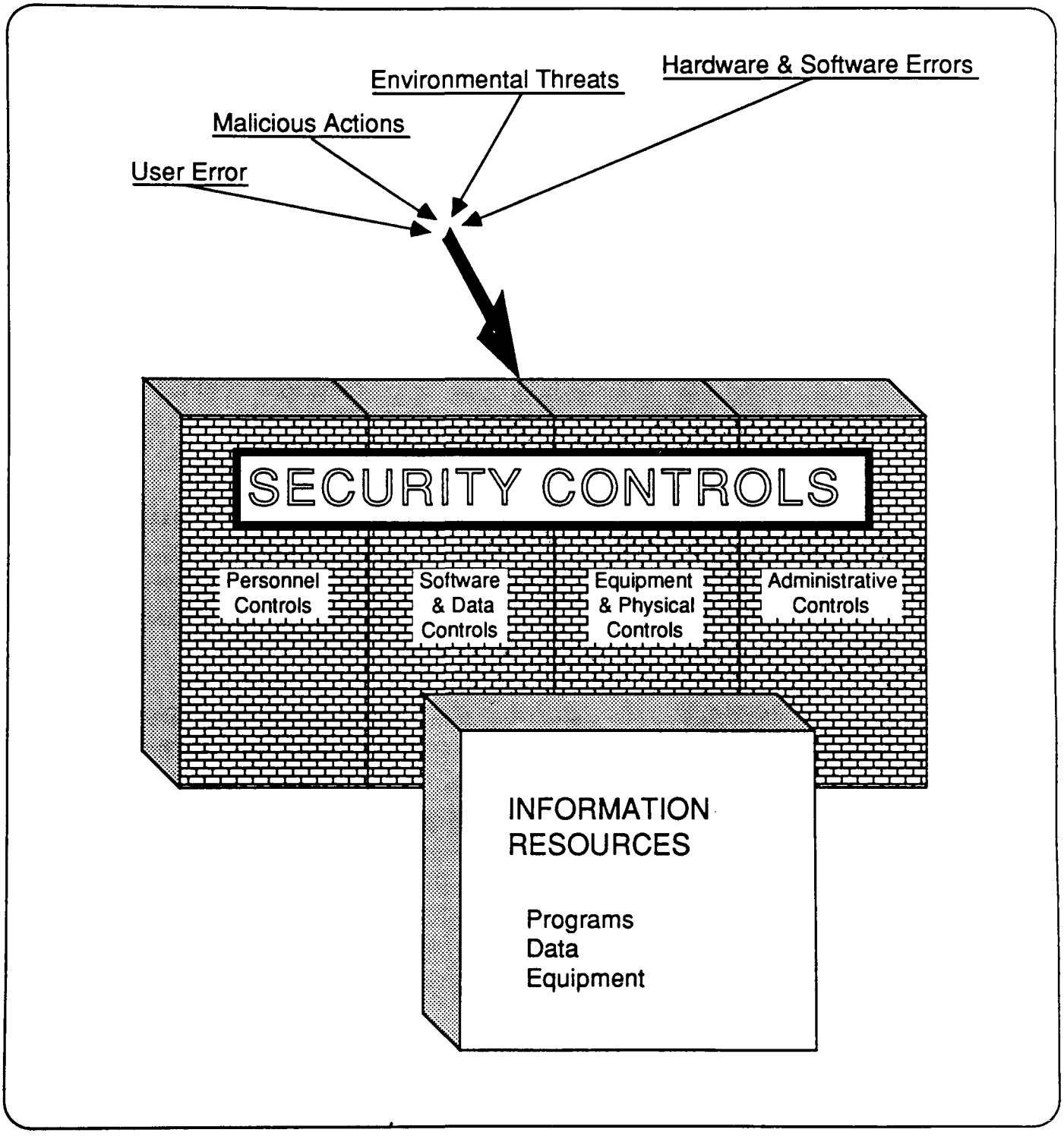
The EPA is highly dependent on its information resources to carry out program and administrative functions in a timely, efficient, and accountable manner. For example, the Agency relies on its information collection authority under various enabling statutes to fulfill its environmental missions. The willingness of the regulated community and state and local agencies to supply requested information in a cooperative and timely fashion depends on their confidence that the information will be adequately protected.

The nature of the information security problem is illustrated in Exhibit 1-2. A wide range of intentional or unintentional events can threaten Agency information resources. These threats include:

- External and environmental threats, such as fire, water damage, or power failure
- Hardware and software error, such as disk or operating system failure for automated information systems
- Operations/procedural error, such as accidental modification or destruction of data
- Malicious actions, such as theft or data sabotage.

EXHIBIT 1-2

THE SECURITY PROBLEM



How vulnerable a particular information resource is to these threats depends on two basic factors. The first is the type or nature of information involved, that is, the relevance of each of the three security objectives. The second factor is the environment in which the information asset is used, for example, is a PC stand-alone or part of a network. Information security involves identifying threats and applying controls to prevent threats from being realized. When threats are realized (for example, disclosure or damage/loss of information), the three security objectives are not achieved.

1.4 STRUCTURE OF THIS MANUAL

Security manuals are typically organized by type of security and include chapters on physical security, data security, and communications security. While such manuals provide good technical discussions of security controls, they typically overwhelm the reader with a hodgepodge of safeguards that leave him/her unclear about exactly which safeguards should be implemented. In addition, these manuals provide little overall implementation guidance.

This manual is structured in a completely different manner. It is organized to allow each reader, whether manager or staff member, to tailor it to his/her own particular security situation. In a very real sense, the manual allows each reader to work through his/her security problem by completing one or two worksheets and by reading selected portions of the text.

Following the introductory material presented in this first section, Section 2 addresses individual and organizational information security responsibilities and is to be read by all EPA managers and staff. Because it is not easy to coordinate the diverse elements of an information security program, Section 2 recommends that one management official, the Senior Information Resources Management Official (SIRMO), be the focal point for information security in each major organizational unit.

Section 3 describes minimal security controls to be used regardless of the type of information involved. Section 3 should also be read by all EPA managers and staff.

Section 4 is the last section that needs to be read by all managers and staff. Section 4 analyzes the need for additional security controls by determining whether or not the reader has a sensitive information asset. Based on the Section 4 determination, the

reader is referred to later sections of the manual as appropriate.

1.5 RELATIONSHIP TO OTHER SECURITY PROCEDURES

In this manual, the Office of Information Resources Management (OIRM) is establishing overall, Agency-wide security procedures for safeguarding EPA information resources. Other EPA organizations have developed specialized procedures in particular information security areas. As an important example, the National Data Processing Division (NDPD) in Research Triangle Park issues technical policies concerning systems (for example, Prime or VAX) supported and approved by it. These policies are contained in the "NDPD Operational Policies Manual." In addition, EPA organizations with statutory authority for certain types of information (for example, the Office of Toxic Substances for TSCA CBI) issue security procedures dealing exclusively with a certain type of information.

Nothing contained in this manual is intended to contradict or replace the specialized security procedures of these other organizations. Those specialized procedures supplement the core procedures presented in this manual. EPA organizations that issue such procedures must ensure that they are consistent with this manual. EPA employees must make sure they adhere to all such specialized procedures, as well as to the procedures presented in this manual.

2. INFORMATION SECURITY ROLES AND RESPONSIBILITIES

2.1 BACKGROUND

Information security involves much more than technical hardware and software issues. Above all, a successful information security program needs strong organizational and administrative controls. Administrative/managerial factors such as top management support and employee awareness contribute significantly to program success. An information security program needs to involve all employees and to be a part of the day-to-day operations of an organization.

Because of these factors, the Information Security Policy assigns information security responsibilities to top management, to supervisors, and to employees. This manual is intended to explain to EPA managers and staff how to comply with these responsibilities without burdening programs and individuals. The remainder of this section describes a suggested overall framework for implementing the Information Security Policy.

The framework of security roles set forth in this section is not mandatory. While programs must meet the requirements of the Information Security Policy, they may find they are able to do so by creating somewhat different roles than those defined here. OIRM recognizes that programs may need to modify the framework to meet unique program needs. The framework is not meant to be inflexible and bureaucratic; instead, its intent is to assist programs and individuals in implementing adequate protection of sensitive information.

2.2 INFORMATION SECURITY ROLES: AN INTRODUCTION

A common problem in information security is determining exactly who is responsible for what aspects of security. In determining accountability for information security, it is extremely useful to start with a framework of owner/user/custodian. Throughout this manual, security actions are cast in terms of this framework, while oversight and coordinating actions are the responsibility of management. The framework is described in detail in the next subsection.

It is important to recognize that there may not always be a one-to-one correspondence between individuals and roles. In other words, at times it may be more efficient to have several individuals share the responsibilities of a role. Again, the framework described here is meant to be a flexible implementation tool.

2.2.1 Owners, Users, and Custodians

These three roles are defined as follows:

- Application (or Information) Owner: The owner of the information is the individual or organization who creates and sponsors it. Ownership involves authority and responsibility for the information, either in a programmatic or administrative sense. For example, the Office of Solid Waste and Emergency Response is the owner of RCRIS. The Office of Administration and Resources Management is the owner of IFMS. The owner determines the sensitivity of the application (or information system), assigns custody of the application, and decides who will be allowed to use the application. Consulting with the custodian as appropriate, the owner specifies and approves security controls and ensures that the application is protected on an ongoing basis. The owner also determines backup and availability requirements and communicates them to the custodian.

- Application (or Information) User: Users are individuals who are authorized by the owner to access an application or collection of information.

- Custodian: Custodians possess (or have physical custody of) ADP equipment or the files housing paper records. For example, for PCs and word processors (WPs), the custodian is the individual to whom the PC or WP is assigned, that is, the person responsible for the equipment in the property management sense. In the minicomputer or mainframe environment, custodians are typically suppliers of information services who possess, store, process, and transmit the information. For certain major applications, the custodial role is shared by OIRM and the National Computer Center (NCC). In these cases, OIRM acts as a "software custodian," that is, OIRM acts as a custodian of the files, databases, libraries, and programs that are stored and processed at NCC.

These roles are not always discrete; the owner can be the principal user and custodian of the information. For example, an individual who develops an end-user application for stand-alone processing on his or her own PC is at once the PC custodian, application owner, and application user.

2.2.2 The SIRMO as Focal Point

Because information security covers a variety of information resources and involves

so many different employees and supervisors, it is important to have one management official in each major organizational unit coordinate the security program for that organization. This individual will serve as a security focal point by identifying all owners, custodians, and users, and by disseminating security-related information throughout the organization. While each Primary Organization Head (as defined in the policy statement) may designate whomever he/she wishes for this coordinating role, the SIRMO is strongly recommended for this function. The designate may delegate portions of this security function (for example, identifying owners) to other knowledgeable individuals in the organization, as long as the Primary Organization Head approves and as long as the coordinating role is retained.

2.2.3 Managerial and Administrative Roles

In addition to owners, users, custodians, and SIRMOs, the implementation of the security procedures in this manual also requires the involvement of several other individuals in eight different roles. The first six of these roles exist at present while the remaining two are unique to the security program.

The eight roles are:

- Primary Organization Head
- First-line supervisors
- PC Site Coordinators
- Records Management Officer (paper and microform)
- Systems Analyst/Application Programmer
- Local Area Network (LAN) System Administrator
- Certifying Official: A management official(s) appointed by the Primary Organization Head. This official certifies that the security safeguards in place for each sensitive application are adequate.
- Minicomputer/Mainframe Security Officer: An official(s) appointed by the Primary Organization Head to be responsible for security at the organization's own on-site computer processing installation(s). The term computer installation covers the range of computer processing capabilities from large scale service center support for multiple users (such as NCC) down to smaller general purpose systems for multiple users or dedicated use (such as Prime or VAX systems). The term does not include personal computer installations.

2.2.4 Tying Roles to Information Assets

It is important to recognize that not all roles apply to all types of information assets. Clearly, the role of Minicomputer/Mainframe Security Officer does not apply to PCs and a PC site coordinator is not relevant for paper record systems. Table 2-1 ties roles to the various types of assets.

2.3 ASSIGNING RESPONSIBILITIES TO THE SECURITY ROLES: IMPLEMENTING INFORMATION SECURITY

Ensuring that information resources are adequately protected involves three different management control processes. First, basic common-sense security measures need to be implemented for ADP equipment, regardless of whether or not it processes sensitive information. Second, an application certification process must be established to determine the sensitivity of each automated application and to certify that the security safeguards for each sensitive automated application are adequate. Third, an installation risk analysis process needs to be established to make sure that the security measures in place at the installation adequately protect the sensitive automated applications stored and processed there. Note that the second and third processes establish a structure of security checks and balances. They approach information security both from an installation or equipment perspective and from an application (or information system) perspective.

Each of the three management control processes is described in more detail below. Table 2-2 lays out the security responsibilities associated with the processes on a role-by-role basis.

2.3.1 Minimal Controls

Section 3 describes the safeguards that need to be in place to ensure the basic physical and environmental protection of ADP equipment and magnetic media. Section 3 also sets forth administrative procedures governing the use of computers and commercial software. Minimal controls for PCs and word processors are implemented by custodians or users as appropriate, with oversight provided by the cognizant PC site coordinator. Minimal controls for minicomputer/mainframe installations are implemented by the Minicomputer/Mainframe Security Officer.

TABLE 2-1

TYING SECURITY ROLES TO INFORMATION ASSETS

	Information Resource or Asset				
	Mini/ Mainframe Installation	PC	WP	Paper/ Microform Records	Software Development/ Maintenance
• Primary Organization Head	x	x	x	x	x
• SIRMO	x	x	x	x	x
• Owner	x	x	x	x	x
• PC/WP Custodian		x	x		x
• Mini/Mainframe Security Officer	x				x
• User	x	x	x	x	x
• Supervisor	x	x	x	x	x
• PC Site Coordinators		x	x		
• Certifying Officer	x	x			x
• LAN Administrator		x			
• Records Management Officer				x	
• Application Programmer/ Systems Analyst					x

TABLE 2-2

IMPLEMENTING A MANAGEMENT CONTROL PROCESS FOR INFORMATION SECURITY: RESPONSIBILITIES BY ROLE

Role	Responsibilities
Primary Organization Head	Implements the organization-wide security program. Designates Certifying Officer(s). Assigns a person the responsibility for information security at each installation.
SIRMO	Coordinates the organization-wide security program. Identifies owners, users, and custodians.
Application (or Information System Owner)	Determines information sensitivity. Assigns custody. Initiates application certification process. Authorizes users. Specifies and approves security controls. Specifies backup and availability requirements. Makes sure users and custodian adhere to security requirements.
PC/Word Processor Custodian	Responsible for the security of his/her equipment. Must implement minimal controls. Performs risk analysis.
Minicomputer/Mainframe Security Officer	Responsible for the security of the equipment at the installation. Implements minimal controls. Performs risk analysis. Establishes disaster recovery/continuity of operations plan. Assists owner in selecting controls during system development/operation.
Application (or Information System) User	Adheres to security requirements of owner.
Supervisor	Reviews application certification form. Ensures employees fully comply with information security responsibilities.
PC Site Coordinator	Ensures minimal controls are in place. Advises owner on application certification process.
Certifying Officer	Certifies sensitive applications. Advises owner on application certification process.
LAN System Administrator	Coordinates the selection of security safeguards for networks.
Records Management Officer	Responsible for ensuring that controls are in place for his/her "manual" record systems.
Applications Programmer/Systems Analyst	Incorporates controls into software. Coordinates selection of safeguards with owner and custodian.

2.3.2 Sensitivity Determination, Automated Application Risk Analysis, and Automated Application Certification

The requirements of the certification process, including the completion of the Application Certification Worksheet, are described in detail in Appendix B. Key elements of the process are summarized below:

- Each Primary Organization Head will designate one or more Certifying Officials for his/her organization.
- Each application/information owner will determine the sensitivity of each of his/her applications or collections of information. This determination will be made in accordance with the instructions set forth in Section 4 of this manual.
- Each sensitive automated application must undergo initial certification and then review or audit leading to re-certification every three years. The certification or recertification process will begin with the application owner's completion of the Application Certification Worksheet. The worksheet will capture basic information on application sensitivity, security specifications, design reviews, and tests of security safeguards.
- When the worksheet is complete, it will be forwarded through the owner's immediate supervisor to the cognizant Certifying Official for approval/disapproval.
- The worksheet will be used by the application owner to communicate the sensitivity of the application and the required security procedures to the users of the application.
- It should be noted that in developing the worksheet, the owner performs a qualitative risk analysis, that is, the owner assesses the relative vulnerabilities and threats to the application and then specifies safeguards.

2.3.3 Installation Risk Analysis Process

All Agency installations, including PCs and word processors, are required to undergo a risk analysis. A risk analysis is a means of measuring and assessing the relative vulnerabilities and threats to an installation. Its purpose is to determine how security safeguards can be effectively applied to minimize potential loss. In everyday terms, risk analysis is a procedure for identifying what could go wrong, how likely it is that things could go wrong, and what can be done to prevent them from going wrong.

There are two accepted methods for performing a risk analysis — quantitative and

qualitative. For all Agency installations, a qualitative risk analysis approach may be used. Simply put, this method handles typical situations quickly and efficiently by combining the analysis of risks with safeguard selection. It consists of the following basic components:

- Determine what information is sensitive and non-sensitive. This determination will be made in accordance with the instructions set forth in Section 4 of this manual. If the installation does not process any sensitive information, the risk analysis is at an end and only minimal controls need to be implemented. If the installation does process sensitive information, categorize the sensitive information, for example, "confidential" sensitive.
- For each category of sensitive information, determine the level of sensitivity, for example, highly confidential.
- Decide on an overall set of safeguards or security controls to use.
- Tie subsets of those safeguards to particular categories of information and to levels of sensitivity.

Implementation of a PC or word processor installation risk analysis is the responsibility of the custodian. Implementation of a minicomputer/mainframe installation risk analysis is the responsibility of that installation's Security Officer. By working through this manual, an informal and qualitative risk analysis will be performed. The custodian or Security Officer need only adhere to the procedures presented in this document and complete the Risk Analysis Worksheet described in Appendix C. No special analytical process has to be undertaken.

Under certain circumstances, PC custodians and Security Officers may feel that more rigorous, quantitative methods are warranted. OIRM does not wish to prohibit quantitative analyses. Interested individuals should review the last section of Appendix C for more information.

2.4 STREAMLINING THE IMPLEMENTATION OF INFORMATION SECURITY

In establishing these management control processes, OIRM wants to achieve adequate security throughout the Agency without unduly burdening programs and individuals. To that end, organizations may find that the following can help streamline the management control processes discussed above:

- In some organizations, one individual (or a handful of individuals) may be knowledgeable enough about an information asset (for example, PCs and

the information contained on them) to function as a composite or aggregate owner, user, and custodian for the asset. In other words, the individual has the requisite knowledge to complete the organization's Application Certification and Risk Analysis Worksheets, not just the worksheets for his/her own hardware and applications. This aggregated approach is consistent with the owner/user/custodian framework and is an acceptable approach to achieving compliance.

- In identifying applications for sensitivity determination and certification, individuals/organizations may find that some applications are subsystems or "children" of larger "mother" applications. Similarly, some applications may be so related that the boundaries between them are fuzzy and that for the purposes of this document they can be thought of as one. In implementing the certification process, such sensitive applications may be combined into a single sensitive application. A key test of whether or not a sensitive application has been properly delineated is whether or not the questions on the certification worksheet can be meaningfully answered. If the responses are full of exceptions and two-part answers, the aggregation is probably incorrect.

2.5 ORGANIZATIONAL SECURITY REPORT

To tie together the diverse elements of its information security program, each major organizational unit (corresponding to each Primary Organization Head) will prepare an annual security report. In establishing this reporting requirement, OIRM wants to make sure organizations are implementing and maintaining security safeguards; OIRM does not want to bog organizations down in a time-consuming paper exercise. To that end, the report will be a compilation of the worksheets and documents prepared during the day-to-day implementation of each organization's security program.

Specifically, the report should contain the following:

- A listing of all sensitive automated information systems in the organization
- Copies of Application Certification Worksheets and Installation Risk Analysis Worksheets prepared in the organization within the past year
- Copies of installation disaster recovery/continuity of operations plans or quantitative installation risk analyses prepared or updated in the last year
- Copies of any local security procedures developed in the last year
- A statement, signed by the SIRMO, that all employees in the organization

have completed basic security awareness training (per Section 5.5)

- Descriptions of any security concerns or weaknesses that the organization may wish to discuss. This could include weaknesses identified as part of audits, vulnerability assessments, or other internal control review processes.

The security report should be sent by the end of each calendar year to the Director, OIRM. The first report will be due at the end of 1990. The report will provide OIRM with evidence of compliance with the security program.

2.6 SECURITY PLANS

The Computer Security Act of 1987 required the EPA to prepare security plans for certain of its applications and computer processing installations. The purpose of the security plan was to provide a basic overview of the security requirements of the subject application or installation and EPA's plan for meeting those requirements. The plan was not intended to be a detailed technical description of risks or security mechanisms. The plans were a new reporting requirement for agencies; they were not designed to replace such existing processes as application certification.

Completed security plans were submitted in FY 1989 to the National Institute of Standards and Technology (NIST) (formerly the National Bureau of Standards) and to the National Security Agency (NSA) for comment and review. Requirements for FY 1990 and beyond have not yet been determined by NIST, NSA or the Office of Management and Budget. Organizations will be informed of any reporting requirements under separate cover.

3. MINIMAL SECURITY CONTROLS FOR MINICOMPUTER/MAINFRAME INSTALLATIONS, PCs, PC LANs, AND WORD PROCESSORS

3.1 INTRODUCTION

This section applies to all individuals with security responsibilities for minicomputer/mainframe installations, PCs, or word processors (such as PC users, PC custodians, LAN Administrators, or Computer Installation Security Officers). This section does not apply to individuals with security responsibilities for paper records or for application system development. Because there are no minimal security controls associated with paper records or application system development, individuals responsible only for these types of assets should skip to Section 4.

The purposes of this section are: (1) to describe the security measures that need to be taken to ensure the basic physical and environmental protection of ADP equipment and magnetic media, and (2) to set forth administrative procedures governing the use of computers and commercial software. All measures described in this section can be implemented at little or no cost, ensuring their overall cost-effectiveness. The emphasis here is on common-sense measures that are justified without a risk analysis. Section 3.2 below deals with PCs and word processors; Section 3.3 addresses minimal controls for minicomputer/mainframe installations.

3.2 MINIMAL CONTROLS FOR PCs, PC LANS, AND WORD PROCESSORS

The responsibility for making sure these controls are in place rests with custodians or users as indicated below. Cognizant PC site coordinators should ensure compliance with these requirements through periodic, informal inspections.

3.2.1 Physical Controls

Agency physical security procedures issued by the Facilities Management and Services Division (FMSD) state that:

> "All office equipment...should be locked up when not in use...Cables and anchor pads can be used to secure typewriters, calculators, computer peripherals, and the like. See SCR 1-08 for information about locking devices." (Directives Volume 4850-1, SCR 1-06, page 7)

Consistent with these procedures, the following controls for PCs and word processors are required to prevent theft and physical damage. Custodians are responsible for ensuring that these controls are in place.

- Locate equipment away from heavily traveled and easily accessible areas to the extent possible.
- When possible, install the device in a locked room, making sure the lock is used whenever the room is unoccupied (and not just at night). If the device cannot be installed in a locked room, a locking device such as a locking anchor pad or hardened cables can be used. For further information or assistance, contact the Security Management Section of FMSD.
- All IBM PC/AT and most compatible microcomputers are delivered with standard system locks which prevent the system from being operated and prevent the cover from being removed, guarding against component theft. Use these locks. When adding valuable expansion boards (such as additional memory or graphics interfaces) to PCs that do not have factory-installed locks, install a cover lock.
- Place equipment and peripherals on stable and secure platforms away from objects that could fall on them.
- Portable PCs require additional security considerations because their portability increases their vulnerability to theft. In addition to the physical security measurers already mentioned, store all portable PCs in a locked cabinet when not in use. For further information or assistance, contact the Security Management Section of FMSD. Assign a person to track the location of the portable PCs on a regular basis, log them out for use to authorized users, and ensure the portable PCs have been returned to the locked storage area when not in use. Moreover, any employee removing a portable PC from an EPA building for official use must have a property pass.

3.2.2 Environmental Controls

Custodians are responsible for ensuring that the following controls are in place:

- PCs and word processors are sensitive to surges in electrical power. To provide protection against current surges, install a surge protection device. Good quality, multi-stage surge protectors are available for under $100.
- Do not install the device in direct sunlight or in a location with extremes of hot and cold temperatures (less than 50 degrees Fahrenheit or greater than 100 degrees Fahrenheit). Do not leave a portable PC in a parked car, which would also subject it to temperature extremes.

- Equipment (and media) are sensitive to contamination from dirt, smoke, or magnetic fields. Do not eat or drink in the immediate vicinity of the equipment and media. In accordance with the Agency's smoking policy, do not smoke in the vicinity of the equipment. (Smoke is drawn into the vents and through the disk units, covering the units with tar. Tar reduces the life of the disk and the read head.)

- To avoid problems from dust and possible overhead water leaks, protect equipment with inexpensive plastic covers when not in use. Install the equipment as far as practical from overhead water pipes or sprinkler heads.

- Control static electrical charges by placing antistatic mats under the equipment or workstation or by using antistatic sprays. (Laundry fabric softeners containing antistatic ingredients can be used for this purpose and they are quite inexpensive when compared to special purpose antistatic sprays.) Because the problem of static electricity is increased when the air is extremely dry, it can be reduced by the use of humidifiers if these are available.

3.2.3 Magnetic Media Controls

At present, virtually all information on microsystems is stored on magnetic media in the following forms:

- Diskettes
- Fixed disks inside the computer
- Cartridge tapes
- Removable disk cartridges (for example, Bernoulli cartridges).

PC and word processor users need to treat the magnetic media with special care. Flexible diskettes are especially susceptible to damage.

- Keep all magnetic media away from all electrical devices and magnets to avoid magnetic fields. This includes magnetic paper clip holders, building passes or credit cards with magnetized strips, PC hard drive units, and telephones. For example, if a diskette is left on a desk and a telephone is placed over the diskette, data on the diskette may be destroyed when the telephone rings.

- Do not flex diskettes. Bending the media can damage its delicate surface and destroy data.

- Store diskettes in their jackets as soon as they are removed from the equipment. The jackets are made of a special material that is intended to

protect the diskette. Cartridge tapes and removable disk cartridges should also be stored in their original containers.

- Never touch the surface of the diskette platter.
- Do not write on a diskette with a pencil or hard-tipped pen. Use only a soft-tipped marker.
- Keep diskettes in a disk file container when not in use. Dust and other particulate materials can scratch and damage the disk.
- To prevent permanent loss of data on the fixed disk drive, all files need to be backed up and the heads need to be parked before a PC is moved. Some portable PCs also may require that the heads be parked and/or a disk inserted into the disk drive when transporting the portable.

3.2.4 Backups

When it comes to making backups of data and programs, it unfortunately seems that experience is the best teacher. A user often needs to lose an important file before he/she realizes the importance of backup.

For certain types of applications (discussed later in Sections 4 and 6), routine and systematic backups are of particular importance and this manual sets forth specific backup procedures. As a minimal control, however, users should be in the habit of regularly backing up their work. While a precise set of criteria for determining how often to make these backups cannot be provided, how active the data file is and how long it took to create are key factors to consider. The appropriate backup media can vary and can include floppy disks, cartridge tapes, removable disk cartridges, or remote hosts such as minicomputers.

Users should note that if they are using their PC as a terminal for processing data and programs stored at another site (such as a minicomputer, LAN file server, or mainframe facility like the National Computer Center), that site may already be backing up the data on a regular basis. Consult the manager of the remote facility or the LAN System Administrator for information.

3.2.5 Software Copyrights/Licenses and Master Copies

Owners and users who purchase commercial software must follow the procedures below. Supervisors are responsible for ensuring that their employees adhere to these procedures.

- Commercial software is typically under copyright and accompanied by a licensing agreement which specifies whether copies may be made. EPA employees must adhere to these licensing agreements; unauthorized duplication of software is strictly prohibited and is not condoned by the Agency under any circumstances. A copyright means that any duplicating, selling, or other distribution of the software for other than backup use by the lawful user(s) is a crime. Willful violations of U.S. copyright law can result in significant penalties (civil damages of up to $50,000 in addition to actual damages plus criminal penalties of up to one year in jail and/or a $10,000 fine).

- In general, there are two types of licenses —single-machine and site. A single-machine license allows the user to install the master copy of the software on his/her machine only. With a site license, the software may be installed on more than one machine, typically for a higher fee.

- Software purchased by EPA must be used exclusively on PCs and word processors owned by EPA.

- Software licensing agreements should be signed upon receipt and immediately filed with the vendor. A copy of the agreement containing the registration number should be filed in a safe place. Returning the agreement to the vendor will register the purchase and may result in free user assistance, free or reduced price software upgrades, and other advantages. Registration of the software will also provide the basis for getting assistance from the manufacturer if the software is lost, stolen, or damaged.

- Existing OIRM procedures concerning master copies of software state that each Primary Organization Head needs to establish a central repository for the organization's master copies to ensure accountability and control. The Washington Information Center (WIC) can be used for this purpose if an organization executes an Operational Service Agreement for Archiving of PC Software.

3.2.6 Unauthorized Use of Personal Computers, Word Processors, and Associated Software

EPA PCs, word processors, and associated software are for official EPA business only. Use of these devices is not allowed for personal business of any kind, even if it is done on the employee's own time. Appropriation of EPA-owned software for personal use, whether done by unauthorized copying or by actual removal of the master software, is prohibited. Training and practice on EPA PCs and word processors should be done using work-related examples. Employees who use this equipment for other than official Agency business are subject to disciplinary action ranging from a reprimand to dismissal.

3.2.7 Non-EPA Software and Viruses

Computer viruses have received a great deal of attention in the press. While some of the coverage is sensational, it is clear that the problem is real and that risk does exist. The threat of viruses has made the need for regular backups (per Section 3.2.4) even greater.

In general, a computer virus is an extra program hidden within an apparently normal program or software package referred to as the virus "host" or "Trojan Horse". Like a biological virus, the computer virus has two important characteristics — it can replicate itself and it can cause harm or mischief. This replicating ability means that a virus can quickly spread via shared diskettes, networks, electronic bulletin boards, or file servers as programs or files are stored, executed, uploaded, or downloaded. Potentially infected host software includes operating system tools such as an editor or file utility, data base management software, or spreadsheet macro languages.

Some viruses are relatively harmless and only flash a message on the monitor before destroying themselves. Others are truly malicious and modify or destroy programs and data. To detect and combat viruses, a number of specialized programs or software "vaccines" have been developed. Because various computer viruses operate in different ways, no single vaccine is currently effective against all of them. Indeed, some of the vaccines have harbored viruses themselves.

Under these circumstances, it is not possible to develop a set of generic, straightforward procedures to ensure the integrity of non-EPA or public domain software. Consequently, EPA employees should not install non-EPA or public domain software on their computers without the express approval of their SIRMO or the SIRMO's designate. In addition, EPA employees and contractors who use PCs or LANs supported and approved by NDPD are also subject to virus prevention policies set forth in the "NDPD Operational Policies Manual." Those policies include recommendations related to new software, backups, and regular checks for program/file size changes.

Readers may also wish to consult the additional guidance presented in NIST Special Publication 500-166, entitled "Computer Viruses and Related Threats: A Management Guide." The publication, which was issued in August 1989, provides general guidance for managing the threats of computer viruses and unauthorized use. It deals with different computing configurations such as multi-user systems, personal

computers, and networks. A copy is available in the EPA Headquarters Library or through the Government Printing Office.

3.3 MINIMAL CONTROLS FOR MINICOMPUTER/MAINFRAME INSTALLATIONS

Computer Installation Security Officers are responsible for making sure the following controls are in place.

3.3.1 Physical Controls

- Locate computer installations away from heavily traveled and easily accessible areas, and away from potential sources of explosions (such as boiler rooms, laboratories, or hot water heaters). When choosing a site, take advantage of existing physical security.
- Avoid locating installations on the ground floor, where an intruder is more likely.
- Install locks on doors and windows. Make sure the lock is used whenever the room is unoccupied (and not just at night).
- Limit the number of entrances to the installation to those needed for effective, efficient operations.

3.3.2 Environmental Controls

- When possible, locate master power switches near emergency exits. The switch should cut all power to the computer system and should also turn off the air conditioning system if it is not designed to filter out smoke. Make sure these master switches are clearly labeled to avoid an accidental power shut-down.
- Mount hand-held fire extinguishers in visible, accessible areas. Use types that will not damage computer equipment, that is, do not use extinguishers that emit water or powder.
- Install smoke and heat detectors.
- Avoid installing the computer room underneath water pipes or steam pipes. If this is not possible, use water sensors to detect water seepage. Store waterproof plastic in a visible, accessible location so that it can be draped over equipment in the event of an emergency.
- Computer equipment (and media) are sensitive to contamination from dirt,

dust, and smoke. Prohibit eating, drinking, and smoking in the computer room. To cut down on dust, avoid coat racks, throw rugs, venetian blinds, and other furnishings that collect dust and static electricity. Vacuum carpeted areas frequently.

- Control static electrical charges by using antistatic carpeting or sprays. Laundry fabric softeners containing antistatic ingredients can be used for this purpose and they are quite inexpensive when compared to special purpose antistatic sprays.

- To reduce fire hazards, never store flammables in the computer room. Keep on-site paper supplies to a minimum.

3.3.3 Configuration Management and Change Control

Because threats can be introduced through unauthorized hardware or software, only Agency authorized hardware and software should be used. Before installation, changes to both hardware and software need to be tested and properly authorized. To help achieve effective configuration management, adhere to the following procedures:

- Maintain accurate records of hardware/software inventories, configurations, and equipment locations.

- Comply with the terms of software licensing agreements. Penalties for violations of U.S. copyright law are set forth in Section 3.2.5 above.

- Adhere to the procedures concerning non-EPA software and viruses that are set forth in Section 3.2.7 above.

More detailed guidance concerning configuration management and change control as they relate to the software life cycle is contained in the EPA "Operations and Maintenance Manual."

3.3.4 Unauthorized Use of Computers and Software

EPA computers and associated software are for official EPA business only. Use of these computers is not allowed for personal business of any kind, even if it is done on the employee's own time. Employees who use hardware and software for other than official Agency business are subject to disciplinary action ranging from a reprimand to dismissal.

4. DETERMINING THE NEED FOR ADDITIONAL CONTROLS

The minimal controls described in Section 3 are always required regardless of information sensitivity. The purpose of this section is to determine whether or not additional controls are necessary.

Application/information owners use this section to evaluate the sensitivity of each of his/her applications or collections of information. Determining sensitivity is an owner responsibility. If sensitive applications/information are owned, later sections of this manual need to be consulted to determine safeguards and to develop the information required for the application certification process and the Application Certification Worksheet (see Appendix B).

Application/information users review this section to develop a working understanding of information sensitivity. Users can also use this section to determine the sensitivity of applications or collections of information not yet evaluated by the owner (for example, existing applications that are undergoing certification). Later sections of this manual should then be reviewed as appropriate.

PC custodians, LAN System Administrators, and Minicomputer/Mainframe Security Officers review this section to develop a working understanding of information sensitivity. They then combine this understanding with owner sensitivity designations to determine the number and type of sensitive applications being processed by users of his/her installation. This determination becomes an input to the risk analysis process outlined in Appendix C.

4.1 DETERMINING SENSITIVITY AND THE TYPE OF INFORMATION

The reader should review Section 2.4 before proceeding. That section contains information on combining applications or collections of information for sensitivity determination purposes.

The questions presented in the sensitivity evaluation table (Table 4-1) are designed to determine whether a particular application or collection of information is sensitive. To use the table, first read through all 11 questions presented in columns (1)-(11) of

TABLE 4-1
TABLE FOR SENSITIVITY EVALUATION

Name of Application/ Information	QUESTIONS											OBJECTIVE/LEVEL		
	(1) National Security Information?	(2) Critical to Performing a Primary Agency Mission?	(3) Life Critical?	(4) Financial Where Misuse Could Cause Loss?	(5) Automated Decision-Making Application?	(6) Subject to the Privacy Act?	(7) Confidential Business Information?	(8) Enforcement Confidential?	(9) Budgetary Prior to OMB Release?	(10) High Value?	(11) Other Sensitive?	Availability	Integrity	Confidentiality
"EXAMPLE"		YES				YES						HIGH	HIGH	MEDIUM

NOTES:

Question (2) Answer YES if disablement or unavailability of the application, or the loss, compromise, or undesired alteration of the information could jeopardize the Agency's ability to perform a primary mission.

Question (3) Answer YES if the loss of information or disruption of the application could jeopardize human life or welfare.

Question (4) Relates to check issuance, funds transfer, etc., where misuse could cause loss.

Question (5) Answer YES if the application makes unsupervised automated decisions based on programmed criteria (for example, issuing checks, ordering supplies, or performing similar asset accounting/control functions) and if the wrong automated decision could cause loss.

Question (10) Answer YES if this is an application/information of "High Value" to the Agency or a particular organization. The term "High Value" must be defined by the owner of the information or application. While a precise set of criteria for determining High Value cannot be provided, the cost of replacing the information and the problems that would result from doing without the information are primary factors to consider.

Question (11) Answer YES if: (1) you answered NO to all other questions, and (2) this is an application/information whose loss would acutely embarrass the Agency, subject the Agency to litigation, or impair the long-run ability of the Agency to fulfill its mission.

the table.

If all questions can be answered "No" for all applications/information, the remainder of this manual does not apply. If any question can be answered "Yes" for any application or collection of information, continue with the instructions in the next paragraph. (After completing the table, make sure to have it reviewed as described in Section 4.3.)

The table has been designed to be a worksheet for evaluating sensitivity. To use the table, list in the first column the name of each application or collection of information for which at least one question can be answered "Yes." For each listed application or collection of information, answer each question. A sample entry is provided. (Leave the last three columns (security objectives) blank for the time being; how to use these columns is explained below.) If more than one type of sensitive information asset is at issue (for example, three sensitive paper record systems and two sensitive PC applications), fill out a separate worksheet for each type of asset.

4.2 DETERMINING RELEVANT SECURITY OBJECTIVES AND THE DEGREE OF SENSITIVITY

The next step is to determine the degree of sensitivity and the relevance of each of the three security objectives. Table 4-2 maps each type of information to its corresponding objective(s) and sensitivity level (that is, high versus medium). (Cases of little or no sensitivity are covered by the minimal controls specified in Section 3.)

For each application or collection of information, determine the relevant security objective(s) and sensitivity level(s) based on the type of information the application/ collection contains. Note that the time value of critical information/applications must be evaluated to determine sensitivity level, and the approximate dollar value of high value information/applications must be estimated to determine sensitivity level. Most life critical and mission critical applications will probably involve high level sensitivity.

It may be helpful to make notes about security objectives and sensitivity levels in the last three columns of the Table 4-1 worksheet. A sample entry is provided. In instances where an application or collection of information turns out to be at both the

TABLE 4-2

DETERMINING RELEVANT SECURITY OBJECTIVES AND DEGREE OF SENSITIVITY

Type of Information	Availability High Level	Availability Med. Level	Integrity High Level	Integrity Med. Level	Confidentiality High Level	Confidentiality Med. Level
• National Security Information					x	
• Critical to Performing a Primary Agency Mission						
-Must be Available Continuously or Within 1 Day	x		x			
-Must be Available Within 1-5 Days		x	x			
• Life Critical						
-Must be Available Continuously or Within 1 Day	x					
-Must be Available Within 1-5 Days		x				
• Financial Where Misuse Could Cause Loss			x			
• Automated Decision-Making Application			x			
• Subject to the Privacy Act						x
• Confidential Business Information						x
• Enforcement Confidential						x
• Budgetary Prior to OMB Release						x
• High Value						
-Very High Value*	x					
-Other High Value		x				
• Other**		x		x		x

While a precise set of criteria for distinguishing between "very high value" and "other high value" cannot be provided, the cost of replacing the information is the primary factor to consider. Clearly, an automated information system that cost $3,000,000 or more to develop and program would be of "very high value."

*** Reader must determine which objectives are relevant based on characteristics of information/application.*

high and medium sensitivity levels vis-a-vis an objective, the higher level dominates. For example, an application that contained both National Security Information (high level confidentiality) and Privacy Act data (medium level confidentiality) would be of high level confidentiality.

By completing the Table 4-1 worksheet, a security profile is developed that includes information on types of sensitive information or applications, security objectives, and sensitivity levels. The security profile contains the basic information owners need to complete the top of the Application Certification Worksheet. It also contains the basic information PC custodians and Security Officers need to complete the top of the Installation Risk Analysis Worksheet.

4.3 VALIDATING SENSITIVITY RESULTS

Determinations of sensitivity and degree of sensitivity must always be reviewed by the cognizant supervisor. Because implementing security safeguards can involve considerable expense and investment of staff time, management review of these determinations is important.

Management review is also important because some of these determinations can involve an element of judgment for which an organizational perspective is important. Critical or high value information is not as easily identified as Confidential Business Information or Privacy Act data. There may be a tendency for individuals to overdesignate their application as critical or high value. SIRMOs should be consulted when employees and supervisors need guidance in making a sensitivity determination.

4.4 USING THE REST OF THIS MANUAL

The next section, Section 5, discusses personnel security. This section needs to be read by all EPA managers and staff who have sensitive applications or information.

The remainder of the manual, Sections 6-10, is organized on an information resource-by-information resource basis, such as PCs or paper records. Within each of these sections, procedures are presented in terms of security objective, for

example, security procedures to maintain high-level availability. Read only those sections and subsections that are applicable. If more than one security objective is applicable (for example, an application where both availability and confidentiality are relevant), make sure to read the subsection pertaining to each applicable objective.

5. PERSONNEL SECURITY AND TRAINING

5.1 INTRODUCTION

Given the large number of Agency information resources, security is as much a people issue as it is a technical issue. SIRMOs need to make sure that cognizant supervisors in their organizations adhere to the following procedures.

5.2 SCREENING AND CLEARANCE

Federal regulations require clearance of all persons involved in the design, development, maintenance, and operation of sensitive automated systems and facilities. These requirements apply to Federal employees and to the personnel of agents (including contractors and grantees) of the EPA who have access to sensitive EPA information. Determinations of the degree of sensitivity of each position are accomplished by the program office. The level of screening required should then vary from minimal checks to full background investigations, depending upon the sensitivity of the information to be handled by the individual in the position and the risk and magnitude of loss or harm that could be caused by the individual. The responsibility for the implementation and oversight of the personnel clearance program rests with the Office of the Inspector General and the Personnel Management Division. EPA organizations should consult with them when obtaining clearances or designating sensitive positions.

5.3 SEPARATION OF DUTIES

An individual has a harder time concealing errors and irregularities if he/she does not control all aspects of an activity or transaction. For example, by separating the functions of cash handling and bookkeeping, the bookkeeper cannot get to the cash and the cash register clerk cannot adjust the books to hide cash shortages.

To the extent possible, the following 11 functions should be assigned to different individuals:

<u>Data Creation and Control Functions:</u>

1. Data collection and preparation
2. Data entry

3. Data base administration
4. Custody of data

Software Development and Maintenance Functions:

5. Applications programming
6. Design review
7. Application testing and evaluation
8. Application maintenance

Administrative Functions:

9. Security planning
10. Security implementation
11. Security audit.

Given the very definition of personal computing, it is often impractical to separate functions for PCs. The same individual often collects data, programs the application, enters the data, and generates the reports. Given the realities of computer-related staffing, it is also sometimes difficult to separate functions in the minicomputer or mainframe environment. To minimize the potential for fraud, abuse, or sabotage, these functions should be performed by separate individuals to the maximum extent practicable. When it is not possible to have each function performed by a different individual, try to separate the following: (1) data creation/control functions from software development/maintenance functions, (2) application programming and maintenance functions from design review and testing/evaluation functions, and (3) security audit from all other functions.

In the case of all financial applications (relating to check issuance, funds transfer, and the like) where misuse could cause loss, separation of functions or duties is mandatory. This separation also applies to financial applications which may be PC-based. For example, the task of preparing payment vouchers must be kept separate from the task of approving payments. For such financial applications, other preventive measures include periodically rotating jobs and asking people to take vacations of one to two weeks. Because the perpetrator of a fraud often has to manipulate accounts on a daily basis to avoid detection, these measures may be a strong deterrent.

5.4 TERMINATION/SEPARATION

In the event an employee must be removed or laid off, it is a good idea to rotate the employee to a non-sensitive position prior to giving notice of the action. While this

may seem extreme, angry and demoralized employees have been known to sabotage programs, erase data bases, or plant computer viruses.

Regardless of the type of separation (resignation, removal, etc.), supervisors need to make sure the following actions are performed for personnel separating from a sensitive position:

- Change or cancel all passwords, codes, user IDs, and locks associated with the separating individual
- Collect all keys, badges, and similar items
- Reconcile any financial accounts over which the employee had control.

The SIRMO or his/her designate should then certify that these procedures have been accomplished by signing and dating a short statement that says: "Information security procedures for separating employee (NAME) have been completed." These statements should be kept on file for inspection by OIRM or the Office of the Inspector General.

5.5 TRAINING

The Office of Administration and Resources Management (OARM) is coordinating the development of a comprehensive information security training program for the Agency to supplement the procedures in this manual. Details and requirements of the program will be issued under separate cover. These requirements will include mandatory basic security awareness training for every employee. The program will include both information security awareness training for all employees and training in accepted security practices for those employees involved in the management, use, or operation of sensitive information. The program will identify and reference, as appropriate, existing training in the information security area, such as training done by NDPD.

6. SECURITY FOR MINICOMPUTER AND MAINFRAME INSTALLATIONS

6.1 INTRODUCTION

This section sets forth security procedures for minicomputer and mainframe installations. Installations of this type cover the range of computer processing capabilities from large scale service center support for multiple users (such as the NCC) down to smaller general purpose systems for multiple users or dedicated use (such as Prime or VAX systems).

Minicomputer/Mainframe Security Officers are responsible for implementing the procedures in this section. Because of the size of WIC and NCC, certain of the procedures below apply only to the Security Officers of those two installations. However, NCC/WIC procedures may also be appropriate for other installations, depending on the results of the risk analyses performed for those installations. Procedures that distinguish between NCC/WIC and other installations will be clearly identified.

The remainder of this section is organized as follows. Because the selection of safeguards or security measures for a minicomputer/mainframe installation needs to begin with a risk analysis, Subsection 6.2 introduces techniques for performing this analysis. Subsection 6.3 introduces a second important technique — disaster recovery and continuity of operations planning. Subsection 6.4 specifies controls that help achieve all three security objectives simultaneously. The last three subsections set forth specific controls for ensuring the availability, integrity, or confidentiality of installation information resources. If more than one objective applies to the installation (for example, availability and confidentiality), make sure to review the subsection for each applicable objective.

The reader must note that NDPD issues technical policies (for example, governing passwords or backup frequency) for systems supported and approved by it. Readers also need to refer to these policies, which are contained in the "NDPD Operational Policies Manual". These policies are typically more hardware specific and technically oriented than the procedures presented here. Security Officers must also comply with NDPD policies when applicable.

6.2 RISK ANALYSIS

As explained in Section 2, each Minicomputer/Mainframe Security Officer must perform a risk analysis for his/her installation. For all installations, a qualitative risk analysis may be used. Detailed procedures for performing the analysis are presented in Appendix C.

Any harm to an installation will manifest itself as a loss of information integrity, a loss of information confidentiality, and/or a loss of processing availability. One of the key outputs of the risk analysis process will be an understanding of the threats (fire, theft, etc.) likely to cause harm to the installation.

In selecting control measures from Subsections 6.4-6.7, Security Officers must always consider the reduction in risk the security measures will achieve. In other words, do not implement the procedures in this section in a vacuum; instead implement these procedures only in conjunction with the Appendix C risk analysis.

6.3 DISASTER RECOVERY AND CONTINUITY OF OPERATIONS PLANNING

Security Officers are responsible for preparing a plan for disaster recovery and continuity of operations for each minicomputer/mainframe installation. Procedures for preparing the plan are presented in Appendix D.

Such plans are particularly important for ensuring the availability of critical or high value Agency applications. To the extent an installation limits itself to confidential or integrity-oriented applications, contingency planning is less important. Appendix D requires a less extensive plan for installations of this type.

6.4 PROCEDURES FOR ALL SENSITIVE INSTALLATIONS

For sensitive minicomputer/mainframe installations, there are a number of controls that help achieve all three security objectives simultaneously. For example, requiring the user to provide a password when logging on to a system can prevent disclosure by denying unauthorized users access to the host computer. The password scheme can also reduce the potential for fraud or sabotage by effectively locking-out unauthorized users. Finally, the chance of accidental data destruction

(a threat to availability) is reduced if inexperienced users are unable to access the host computer due to password protection.

Universal controls of this type fall into four broad categories: (1) hardware controls, (2) software controls, (3) procedural controls, and (4) communications controls. All four categories are discussed below.

6.4.1 Hardware Controls

Many important security safeguards can be built into hardware. Hardware-based protection mechanisms are often cost-effective because they can be applied to so many different information systems and files. By way of contrast, most application-based controls are limited in usefulness to the one application. Hardware-based controls are also typically more difficult to circumvent.

To determine what hardware security features are standard and what features can be obtained at additional cost, contact the appropriate vendor representative.

From a security perspective, the following hardware features need to be implemented when they are available and cost-effective:

- User Isolation: This is the capability to isolate users from each other.
- Alarm: An audible alarm notifies the computer operator when certain events occur, such as an unauthorized access attempt.
- Identifiable Remote Terminals: This is the capability of knowing the identity of remote terminals. This feature augments a password scheme which authorizes each user. With terminal identification, an intruder must have a valid password and access to a valid terminal.
- Error Detection During Processing: This feature involves checking for errors each time memory is accessed. The error checks typically take the form of parity and address bounds checks. Error detection is particularly useful for maintaining integrity.
- Memory Access Control: This capability limits each user to the memory of his/her own partition.
- Privileged Command Control: With this feature, certain commands are only executed when the computer is in a master or executive mode (as opposed to a user mode). Commands of this type include input/output instructions and partition transfers, and are generally available only to operators or system programming personnel.

6.4.2 Software Controls

The following controls need to be implemented using the operating system and other system software (unless they have already been built into the hardware):

- User programs must be prevented from executing privileged instructions.
- Users must be isolated from each other.
- Hardware and software error logs need to be maintained.
- Error checking needs to occur each time memory is accessed.
- Atypical occurrences that may indicate a security violation need to be recorded. These include unlocking terminals via operator overrides or access failures, such as incorrect passwords.

In addition, the operating system must control the following functions:

- Information transfers between the main memory and on-line storage, and between the central computer and remote equipment
- All functions that allocate ADP resources, such as memory or peripherals
- Utilities and programs that maintain and change the operating system.

6.4.3 Procedural Controls

- Memory dumps must be limited to a user's memory partition. System memory dumps need to be strictly controlled.
- When installation size warrants it, maintain a storage location and a library system for tape and disk storage.
  - Only the media librarian or individuals authorized by the installation's Security Officer will be allowed access to the storage location.
  - All media not scheduled for use within the next day should be stored in the library.
  - Mark each item with a serial number.
  - Keep a record of each item that includes its sensitivity designation, age, frequency of usage, owner, and cleaning schedule.
- Maintain console logs and operating logs.

6.4.4 Communications Controls

Host-level password protection is required for any on-line access to the computer. (Host-level passwords are those used when first logging on to the computer system, for example, VAX or IBM Mainframe.) In implementing password protection, make sure of the following:

- Passwords are at least six characters in length.
- The password must contain at least one alpha and one numeric character.
- Passwords can be deleted or changed in a straightforward, controlled fashion. Passwords are changed at least quarterly.
- Consecutive password failures are limited to no more than four before a user is revoked from the system.
- Passwords are not composed of names or similar personal types of information.

6.5 ADDITIONAL PROCEDURES TO MAINTAIN AVAILABILITY

6.5.1 Procedures for Medium-Level Availability

6.5.1.1 Backups and Continuity of Operations

In general, the most important step to be taken to protect information availability is to implement a regular schedule of backups. If information has been backed up and if the backup has been safely stored, the information will be recoverable no matter what happens. Procedures for backup, disaster recovery, and continuity of operations are contained in Appendix D.

6.5.1.2 Power Protection

Provide for adequate power to guard against fluctuations and failures through the use of surge protectors. Consider implementation of an Uninterruptible Power Supply (UPS) to avoid system failure during brief power disruptions.

6.5.1.3 Physical Access Control

NCC and WIC must maintain a physical access control that includes at least one of the following: key cards, magnetic card locks, remote controlled locks, or closed-circuit television. At night, this system must be supplemented with either an intrusion

alarm or a guard patrol.

Other installations must, at a minimum, maintain a list of personnel authorized to enter the installation. At night, this must be supplemented with a guard control. More rigorous access control systems are acceptable for other installations if they are cost-effective.

6.5.1.4 Visitor Control

All visitors must log-in/log-out and be escorted during the visit.

6.5.1.5 Fire Control

WIC and NCC must install a centralized fire suppression system.

6.5.2 Procedures for High-Level Availability

Follow all procedures set forth in Subsection 6.5.1. In addition, install an emergency power standby capability.

6.6 ADDITIONAL PROCEDURES TO PRESERVE INTEGRITY

To maintain medium level integrity, adhere to the procedures in Subsection 6.5.1 above. To maintain high level integrity, adhere to the procedures in Subsection 6.5.2 above.

6.7 ADDITIONAL PROCEDURES TO PRESERVE CONFIDENTIALITY

6.7.1 Procedures for Medium-Level Confidentiality

6.7.1.1 Control Hard-Copy Reports and Output

Control the production and distribution of confidential output. Keep such output in a locked cabinet or room when not in use. Establish safeguards to prevent confidential reports from being misrouted.

6.7.1.2 Encryption

Some application system owners may determine that encryption is a needed security control when transmitting confidential data. The NCC will provide encryption where required upon request. Other installations may also provide encryption if it is cost-effective, but they must consult with the NCC regarding potential technical and logistical problems.

6.7.1.3 Physical Access Control

See Subsection 6.5.1.3.

6.7.1.4 Visitor Control

All visitors must log in/log out and be escorted during the visit.

6.7.1.5 Disposal Practices

Shred confidential reports when they are no longer needed. Make sure that confidential data are erased from magnetic tapes before releasing them as work tapes, etc. Assist application system owners who wish to erase confidential data from their disk space before releasing it for other uses.

6.7.2 Procedures for High-Level Confidentiality

The EPA has only one type of information in this category - National Security Information (NSI). The amount of NSI possessed by the Agency is extremely small and the need to computerize any of it would be very infrequent.

Because of the small quantity of NSI in the Agency and because NSI involves special security considerations (emanations security and TEMPEST devices), NSI should not be placed on computers without the express approval of the Director, OIRM.

7. SECURITY FOR PERSONAL COMPUTERS AND PC LANs

7.1 BACKGROUND

This section applies to personal computers (PCs) only. A single PC installation is generally comprised of a microprocessor, a video monitor and various peripheral devices for entering, storing, transmitting and printing data. The PC installation may process in isolation as a standalone personal tool and/or it may function as a smart terminal in a communications configuration (such as PC to mainframe). This section does not apply, however, to other types of microsystems such as Lexitron word processors (see Section 8) or dumb terminals (those that are not programmable).

The expanding use of personal computers is creating major new opportunities for productivity improvement at the EPA. At the same time, however, this expanding use of personal computers is placing new information security responsibilities on office managers, research personnel, and others not previously considered to be information processing professionals. This decentralized processing of Agency information means that mainframe and minicomputer processing installations can no longer be relied upon to protect all automated Agency operations.

Certain PC characteristics pose special problems in information security. In general, these include the following:

- Personal computer systems software is typically rudimentary and affords little protection to information and programs.
- Personal computers typically lack the built-in hardware mechanisms needed to isolate users from each other and from certain system functions (such as reading and writing to memory).
- PC information is typically in the form of reports, spreadsheets, lists, and memoranda. These relatively final forms mean that PC data are more readily accessed and understood by unauthorized users than are data in larger computer systems.

7.2 DETERMINING THE PROCESSING ENVIRONMENT; RELATIONSHIP TO OTHER PROCEDURES

Several of the procedural controls specified in Subsections 7.4-7.6 are presented in terms of the environment in which the application or information is being processed. In using those subsections, be alert to procedures that depend on three key environmental characteristics, which can be defined by answering the following questions:

- Is the PC a single-user device or is it shared among multiple users?
- Is the information/application stored on removable media (like a floppy disk) or non-removable media (like a fixed disk) or both (like a fixed disk with a floppy disk backup)?
- Does the PC process in isolation or does it communicate with other hardware? If it does communicate, which of the following communication configurations applies:
  - Remotely accessible by modem (dial-up capability)?
  - PC to resource server?
  - Local area network (LAN)?

Regarding LANs, LAN System Administrators must note that NDPD issues policies (for example, governing access control or backup frequency) for Agency LANs. These policies are contained in Section 310 of the "NDPD Operational Policies Manual." These policies are typically more detailed and technically oriented than the core procedures presented here. LAN System Administrators must make sure that they comply with applicable NDPD policies.

7.3 USING THE REST OF THIS SECTION

The remainder of this section is organized by information security objective. Consult completed Table 4-1 to determine which security objective or objectives are relevant.

- If availability is a security objective, review Subsection 7.4
- If integrity is a security objective, review Subsection 7.5
- If confidentiality is a security objective, review Subsection 7.6.

In discussing procedural controls, Subsections 7.4-7.6 reference hardware and software security products that are available under the PC contract. Information on products and prices was current as of December 1989. Because the Agency periodically updates contract offerings and prices, the reader should consult with his/her PC site coordinator prior to placing an order.

7.4 MAINTAINING INFORMATION AVAILABILITY

7.4.1 Introduction

This subsection sets forth security procedures for owners, users, LAN System Administrators, and custodians of applications of high-level and medium-level availability (as determined in Section 4). This section is to be used as follows:

- Owners develop the security specifications and the tests needed for application certification based on the procedures presented here.
- Users make sure they are in compliance with owner security specifications based on these procedures. In addition, users may consult these procedures when an owner has designated an application as sensitive, but has not yet identified his/her security specifications.
- Custodians and LAN System Administrators use these procedures to make sure that applications can be recovered in the event of a processing disaster and can be run elsewhere if necessary. They also use these procedures to develop the information required for the risk analysis outlined in Appendix C.

The remainder of this subsection is organized as follows. The next part catalogs and describes specific threats to information availability. Subsections 7.4.3 and 7.4.4 specify security measures for medium availability applications and high availability applications, respectively. The last part describes some steps that can be taken to recover from a processing disaster.

7.4.2 Threats to Application and Information Availability

Specific threats to data availability include:

- Theft
- Damage to magnetic media
- Hardware failure: inability to restart

- Hardware failure: failure during use
- Accidental data destruction or other operator errors
- Sabotage (deliberate data destruction)
- Failure of users to back-up data and programs.

The threats of theft and damage to magnetic media were addressed in Section 3. The remaining threats are described below.

7.4.2.1 Hardware Failure: Inability to Restart

Because of the generally high reliability of microcomputers, users tend to become overconfident and to not protect themselves from system failures.

In some cases, microcomputer systems are incapable of being restarted (booted) because of a hardware failure.

If the inability to start the system is caused by a failure of the hard disk drive subsystem and it is necessary to repair or replace the drive, the data on the drive will probably be unavailable after the system has been repaired.

7.4.2.2 Hardware Failure: Failure During Use

Although microcomputers do not often break down, the hardware can fail during use for a variety of reasons. The most common problem is a disruption or surge of electric power, but the failure of almost any internal component can cause the system to crash.

In addition to the problems that may be encountered if the system cannot be booted, failure during use will result in a disruption of ongoing processing. If the system crashes while in use, all data in the volatile, random access memory (RAM) will be lost. In addition, if data files are open at the time of the failure, they may be corrupted.

7.4.2.3 Accidental Data Destruction

The most common way that data are accidentally destroyed is by users issuing incorrect commands. For example, it is possible for users to destroy all of the data on a disk by inadvertently reformatting it. This can be especially damaging if the hard disk is reformatted. Files can also be inadvertently deleted. It is also possible to copy a file on top of an existing file if the name of the existing file is used as the destination

of a copy command.

Data can also be accidentally destroyed by software malfunctions or incompatibility. A particularly serious potential problem is caused by an incompatibility between versions 2.x and 3.x of PC/MS DOS. Specifically, if a system containing a 20mb or larger fixed disk formatted under version 3.x of DOS is booted from a diskette that contains a 2.x operating system, the File Allocation Table of the hard disk will be damaged when data are written to the hard disk. If this happens, it might not be possible to access data stored on the hard disk.

7.4.2.4 Sabotage

Data can be deliberately destroyed by malicious individuals, who may be either authorized or unauthorized users. Such destruction can be the result of vandalism by those outside the office, but it can also be an act by an employee who has been dismissed or disciplined, an act by an individual who is hostile to the mission of an office, or an act by an individual hostile to the implementation of a new computer system. Examples include:

- An employee may oppose the implementation of performance monitoring software.
- An individual may use the data overwriting programs in PC utilities packages to erase files or disks.
- An individual may feel that the automation of the individual's duties may make him or her more expendable.
- A dismissed employee may plant a "virus" in an organization's software prior to departure.
- An individual may believe that the implementation of a system intended to make his or her job easier will actually make his or her job more difficult.

7.4.2.5 Failure to Backup Data and Programs

When it comes to regular and systematic backup, it unfortunately seems that experience is the best teacher. A user often needs to lose an important file before he/she realizes the importance of backup. Failure to perform regular backups is probably the most common and the most serious threat to availability.

7.4.3 Procedures to Maintain Medium-Level Availability

This part applies to applications that can be unavailable for a period of only one-to-

five days and/or applications that are of other high value.

7.4.3.1 Lock-up Media

To avoid theft, store media in a locked cabinet or room.

7.4.3.2 Write Protection

Whenever possible, write-protect files and programs to avoid accidental destruction.

7.4.3.3 Isolated Storage

Isolate the critical/high value application on its own storage media to the extent possible. For an application residing on a floppy disk, this means dedicating the disk to the one sensitive application. For an application residing on a fixed disk, this could mean dedicating a separate subdirectory or partition to the software. Such isolation speeds the backup process (discussed below).

7.4.3.4 Backups

In general, the most important step to be taken to protect information availability is to implement a regular schedule of backups. Backups are performed to provide for easy recovery from a disaster. If information has been backed up and if the backup is safely stored, the information will be recoverable — no matter what happens. Note, however, that transactions that have occurred since the last backup may have been lost and may need to be re-input.

DATA BACKUPS

Each PC user needs to establish a backup loop to protect his/her data and files. The backup loop is a systematic way of creating multiple generations of copies. The frequency and number of backup generations made and stored should be a direct function of the value of the information and the cost of regenerating it. In general, two to five generations are recommended. Two examples involving diskettes are provided below.

- A two-generation scheme for a floppy disk would be performed as follows:
  - On the first day, the data on the original diskette would be copied on to diskette 1.
  - On the second day, the data on the original diskette would be copied on to diskette 2.
  - On the third day, the data would be copied on to diskette 1, over the backup from the first day.

- A five-generation scheme for a fixed disk system would be performed as follows:
  - On Monday of the first week, the user's data on the fixed disk would be copied to a set of diskettes designated as set 1.
  - On Tuesday, the data could be copied to set 2. Wednesday's backup would be copied to set 3, Thursday's to set 4, and Friday's to set 5.
  - On Monday of the second week, the data would be copied to set 1, over the Monday backup from the previous week.

Under a five-generation scheme, the user has a significant level of protection. Even if the original data and one or two of the backups were destroyed, only one or two days of work would be lost.

The backup loop does not have to involve diskettes. As discussed below, tape backup systems or Bernoulli boxes can be more efficient. Moreover, if the PC is connected to a LAN file server or remote host (such as a mainframe computer), the remote device may provide backup protection. Consult the manager of the remote facility or the LAN System Administrator for information.

Backup copies stored in the general vicinity of the original data protect against problems such as a system crash or an accidental erasure of data. They do not, however, protect against a threat such as a fire which could affect an entire floor or building. As a result, each month a copy should be taken out of the backup loop and stored in a physically separate location. This archival copy would probably not be completely current in the event of a major disaster, but it would have great data recovery utility. To prevent archival copies from piling up, the copy that has been in archives can replace the one taken out of the backup loop. There may also be advantages in retaining several generations of archival copies.

For Headquarters employees, the WIC is recommended as an "off-site" location. The WIC does charge a fee for storing backup copies. Participating organizations execute an "Operational Service Agreement for Archiving of PC Software" with the WIC. If the PC is connected to a remote host or file server, it may be possible to use the remote device as the off-site location. Consult the manager of the remote facility or the LAN System Administrator

for assistance.

When files get large, users are tempted to employ the incremental backup approach. An incremental backup focuses only on what has been changed and includes only those files that have been modified since the last backup. The advantage of an incremental backup is that it can be performed faster than the full backups discussed above. The disadvantage of incremental backups is that no single backup will contain all of the files and data. If the original files are destroyed or lost, it will be necessary to reconstruct the data from the most recent full backup and all of the incremental backups that have been performed since. In addition to being inconvenient, this process of reconstructing the files is risky. If the last full backup or any of the incremental backups has anything wrong with it, it may be impossible to perform a fully successful recovery.

Because of these difficulties, incremental backups are not recommended. Instead, if the data files are so large that the backup process fills about 15 diskettes, consider using a streaming tape backup system or a Bernoulli box. A streaming tape backup system is available under the PC contract for about $500. The Bernoulli box, which is available for about $800 (10 megabyte) or about $1200 (20 megabyte) under the PC contract, makes backups straightforward and quick. It also provides certain access controls, for example, partitioning software. If the PC is also used for confidential processing, the box becomes more cost effective. In addition, if software as well as data are stored on Bernoulli disks and a second PC with a Bernoulli box is available, each PC can be a backup facility for the other.

SOFTWARE BACKUPS

Backups should not be limited to data and files. End user applications (software developed or maintained locally) should also be backed up and stored at the off-site storage facility. Source program files, loadable versions of all software, and required compiler or interpreter programs should be included.

7.4.3.5 Continuity of Operations

Backup computing facilities shall be identified for critical applications and an agreement for the use of the backup facility shall be executed. The agreement for

the backup facility should not be an informal and vague oral agreement, but instead must involve a memorandum between the PC custodians identifying all conditions (for example, the amount of machine time to be made available).

7.4.4 Procedures to Maintain High-Level Availability

This part applies to applications that must be available continuously or within one day and/or applications that are of very high value. All procedures set forth in Subsection 7.4.3 also apply here. In addition, the following additional procedures will be adhered to.

7.4.4.1 Uninterruptible Power

Obtain an Uninterruptible Power Supply (UPS) device to provide virtually complete surge protection, a filter for line noise, and power in the event of an outage. A UPS is available for approximately $1100 under the PC contract.

7.4.4.2 Manual Fallback

Identify and formalize manual procedures to be followed in the event of a complete disaster.

7.4.4.3 More Frequent Backups

Consider preparing full backups for off-site storage on a weekly or even daily basis.

7.4.5 Suggestions for Recovering from a Disaster

In the event of a problem or disaster, it is often best to stop using the PC and seek help from the PC Site Coordinator. The following may then help restore availability:

- It may be possible to recover data stored on the undamaged portions of the damaged medium using the DOS DEBUG facility or some other hexadecimal editor. This will be a difficult task and should only be undertaken by individuals with a thorough understanding of their systems.

- Commercially available utility packages (such as the Norton Utilities package available under the PC contract for about $100) can help in recovering data and in unformatting an accidentally formatted disk.

- If backups have been made, data and software that are not copy-protected can be restored from the backups. Contact the manufacturers of copy-protected software to investigate their policy for replacing damaged software.

- If summary data have been damaged, but detailed records or other audit trails were undamaged, it may be possible to recreate the summary data from the detailed records. In some cases it might even be possible to recreate detailed records if sufficient audit trail information is available.

7.5 PRESERVING INFORMATION INTEGRITY

7.5.1 Introduction

This subsection sets forth security procedures for owners, users, LAN System Administrators, and custodians of applications of high-level and medium-level integrity (as determined in Section 4). This section is to be used as follows:

- Owners develop the security specifications and the tests needed for application certification based on the procedures presented here.
- Users make sure they are in compliance with owner security specifications based on these procedures. In addition, users may consult these procedures when an owner has designated an application as sensitive, but has not yet identified his/her security specifications.
- Custodians and LAN System Administrators use these procedures to determine what security measures must be in place at his/her installation to maintain integrity. They also use these procedures to develop the information required for the risk analysis outlined in Appendix C.

The remainder of this subsection is organized as follows. The next part catalogs and describes specific threats to information integrity. Subsections 7.5.3 and 7.5.4 then specify security measures for applications of medium-level integrity and high-level integrity, respectively. Finally, the last part describes some steps that can be taken to recover from data corruption.

7.5.2 Threats to Integrity

7.5.2.1 Deliberate Distortion of Information: Fraud and Sabotage

Data integrity can be damaged by the deliberate actions of system users or other individuals with access to the system. Such damage could take the form of a virus. These actions could be motivated by revenge (for example, by recently disciplined or reprimanded employees) or could be intended to perpetrate or cover up fraudulent activities, mismanagement, or waste.

Fraudulent activities include embezzlement or any other deception intended to cause the deprivation of property or some lawful right. Fraud could be intended to prevent or influence enforcement actions or other operations of the Agency.

7.5.2.2 Accidental Damage

Accidental damage to data integrity results when individuals inadvertently and unknowingly modify data, erase files, input incorrect data, or introduce program bugs.

Accidental threats to data integrity overlap with the issues discussed under data availability. The distinction is based on whether the data distortion is discovered. If so, the distortion would be generally be considered to consist of a loss of data and would therefore be considered to be a data availability problem. When the damage remains undetected, decisions may be made or other actions may be taken based upon incorrect information, resulting in a failure of data integrity.

7.5.2.3 Other Considerations

In addition to the above, information integrity can also be affected by flaws in software applications design and development (for example, incorrect algorithms or mathematical formulae). A review of all system design issues that are relevant to data integrity is beyond the scope of this manual. Instead, the reader is referred to the three volume set of "EPA System Design and Development Guidance" issued by OIRM. This comprehensive set of standards includes references to security at appropriate points in the software design/development process. For more explicit guidance on designing security into applications, the reader is also referred to Federal Information Processing Standard (FIPS) 73 and to Section 9 on application system development. FIPS 73 is available in the EPA Headquarters library or through the National Technical Information Service.

This section will limit itself to a consideration of threats to data integrity involving deliberate and accidental actions of users and involving other events that can occur during system use.

7.5.3 Procedures to Maintain Medium-Level Integrity

The security measures needed to ensure integrity represent a mix of those associated with maintaining availability and those associated with preserving confidentiality. Availability and confidentiality are almost opposites; backup copies of a data

base made to enhance availability can aggravate the problem of preventing the disclosure of data stored in the data base. In a very real sense, however, integrity is the objective in the middle.

Integrity involves elements of the availability objective because if data are corrupted or partially destroyed, intact backup copies are essential. On the other hand, integrity involves elements of the confidentiality objective because preventing fraud and sabotage are largely problems of controlling access.

7.5.3.1 Availability-Related Procedures

Adhere to the procedures described in Subsection 7.4.3, with the exception of those associated with continuity of operations. This will ensure that backups are created.

7.5.3.2 Confidentiality-Related Procedures

Adhere to the access control procedures described in Subsections 7.6.3.2 and 7.6.3.3. Also, follow the password management practices outlined in Subsection 7.6.3.1. In addition, for PCs in a local area network (LAN), adhere to the procedures outlined in the following two paragraphs.

In a LAN, all points can read traffic on the network. In addition, all points have access to common storage media. Indeed, the ability to share printers or storage (file servers) is often a primary reason why networks are created.

The LAN System Administrator is responsible for coordinating the selection of security safeguards for the network to ensure overall effectiveness. LANs sometimes have security packages available as part of their operating systems. These may be considered in selecting safeguards for the network. If all network users have access to all information processed on the network, establish a formal list of those authorized users (an administrative control). To the extent possible, bolster this administrative control by keeping each PC on the network under lock and key when not in use. Require users to provide a password when logging on to the network.

7.5.3.3 Audit Trails and User Accountability Tracking

If fraud and sabotage are threats, audit trails and operator tracking should be incorporated into the application software. The software should be designed to automatically insert the operator identifiers into each record based upon a password supplied during the system sign-on process. Data integrity and user accountability would be

further enhanced if the application software and data base were compiled and encrypted to prevent the password and accountability tracking mechanism from being bypassed.

7.5.4 Procedures to Maintain High-Level Integrity

All procedures set forth in Subsection 7.5.3 above also apply here. In addition, the procedures listed below will be followed.

7.5.4.1 Uninterruptible Power

Obtain an Uninterruptible Power Supply (UPS) device to provide virtually complete surge protection, a filter for line noise, and power in the event of an outage. A UPS is available for about $1100 under the PC contract.

7.5.4.2 Manual Fallback

Identify and formalize manual procedures to be followed in the event of a complete disaster.

7.5.4.3 More Frequent Backups

Consider preparing backups for off-site storage on a weekly or even daily basis.

7.5.5 Suggestions for Recovering from a Disaster

In the event of a problem or disaster, it is often best to stop using the machine and seek help from the PC Site Coordinator. The following may then help restore integrity:

- It may be possible to recover data stored on the undamaged portions of the damaged medium using the DOS DEBUG facility or some other hexadecimal editor. This will be a difficult task and should only be undertaken by individuals with a thorough understanding of their systems.
- Commercially available utility packages (such as the Norton Utilities package available under the PC contract for about $100) can help in recovering data and in unformatting an accidentally formatted disk.
- If backups have been made, data and software that is not copy-protected can be restored from the backups. Contact the manufacturers of copy-protected software to investigate their policy for replacing damaged software.

- If summary data have been damaged, but detailed records or other audit trails were undamaged, it may be possible to recreate the summary data from the detailed records. In some cases it might even be possible to recreate detailed records if sufficient audit trail information is available.

7.6 PRESERVING INFORMATION CONFIDENTIALITY

7.6.1 Introduction

This subsection sets forth security procedures for owners, users, LAN System Administrators, and custodians of confidential applications and information. This section is to be used as follows:

- Owners develop the security specifications and the tests needed for application certification based on the procedures presented here.
- Users make sure they are in compliance with owner security specifications based on these procedures. In addition, users may consult these procedures when an owner has designated an application as sensitive, but has not yet identified his/her security specifications.
- Custodians use these procedures to determine what security measures must be in place to protect the confidential information being stored and processed by users of his/her installation. They also use these procedures to develop the information required for the risk analysis outlined in Appendix C.
- LAN System Administrators must note (per Section 7.6.3.3) that no confidential data may be loaded on to a LAN or made available via a LAN unless specifically approved in writing by the Director, OIRM.

The remainder of this subsection is organized as follows. The next part catalogs and describes specific threats to confidentiality. Subsections 7.6.3 and 7.6.4 specify security measures for applications of medium level confidentiality and high level confidentiality, respectively. Features of the processing environment are particularly important for preserving confidentiality and are discussed in those subsections as appropriate.

Unlike Subsections 7.4 and 7.5, there is no separate discussion here of steps to recover from a breach of confidentiality. Once information has been disclosed, there is little the individual can do to remedy the situation. Instead, the breach must be reported to appropriate Agency officials, as described in the Information Security Policy.

7.6.2 Threats to Application and Information Confidentiality

Specific threats to information confidentiality are largely problems of access control. Note that the threats described below apply to confidential information in its various forms, that is, in the computer, in hard copy, on removable media like diskettes, and on printer ribbons.

- Magnetic media containing confidential data can be accessed by individuals from whom the data should be restricted. If the computer is not in a secure area, intruders can start the system containing the information and browse information on the fixed disk. If diskettes containing confidential information are not secured, unauthorized individuals can install them on a computer and browse their contents.

- Unauthorized individuals could see data on a computer screen or printout if confidential data are processed in an unsecured area or if printouts are not protected in storage.

- Confidential data can be deciphered from printer ribbons used to print confidential reports.

- Unauthorized individuals could access confidential data across a local area network or other communications device if confidential data are stored or processed on a microcomputer that can be accessed remotely.

- Files erased from a magnetic disk using only the standard DOS "DEL" or "ERASE" commands are not actually erased from the computer disk—they are only marked for deletion and the space on which they are written is freed for use by later files. For this reason, until they have been overwritten, they can be "unerased" using commercially available utility programs.

- Some software systems use work files that are temporarily stored on disk. Although the systems usually delete these files when they are finished with them, the deleted files may be recoverable using commercially available utility programs. Similarly, information could be left in the volatile (RAM) memory of the computer if the computer is not turned off after confidential data have been processed.

- Individuals authorized to access confidential information could deliberately share printed reports or magnetic media containing confidential data with unauthorized individuals.

7.6.3 Procedures to Preserve Medium-Level Confidentiality

Preserving confidentiality involves controlling access to information and applications. How easy or difficult it is to control access is highly dependent on the three

key environmental characteristics (single user versus shared, stand-alone versus communicating, removable versus non-removable media). The simplest situation consists of a single user who does stand-alone processing and stores all confidential information on floppy disks. When the PC is shared or in a communicating configuration, the security situation becomes more complicated.

The procedures which follow are presented largely in terms of processing environment. Following a short subsection on controls which apply to all environments, more complicated environments are discussed. The security controls required fall into the following categories:

- Physical, such as door locks
- Administrative, such as lists which specify who is allowed access to a given PC
- System-based, such as password protection
- Information-based, that is, rendering information unusable (even if it is obtained by unauthorized individuals) through scrambling or encryption techniques. As an example, some commercial software (for example, Lotus 1-2-3 Version 2) contain data encryption capabilities. The Lotus 1-2-3 data encryption capability enables users to password-protect their Lotus spreadsheets. The encrypted spreadsheets cannot be accessed without the assigned password and data in them are encoded to prevent the data files from being read through DOS functions or other utilities.

It should be noted that EPA organizations with statutory authority for certain types of confidential information may issue security procedures dealing exclusively with a particular type of information (for example, TSCA or FIFRA CBI). Because of statutory requirements, some of those procedures may be more stringent than those required here. EPA employees must make sure that they also adhere to such organizational standards and procedures.

7.6.3.1 Procedures for all Environments

- Discourage traffic in the area where the computer is located when in use. Unauthorized individuals should be kept out of the area so that they cannot view data that might appear on the computer screen.
- Log off or otherwise inactivate the PC whenever leaving it.
- Store hard-copy reports and removable media containing confidential data in locked cabinets or rooms.
- Printer ribbons used to print confidential data should be considered confidential as well. Destroy exhausted ribbons so that they cannot be

deciphered by an unauthorized individual.

- Be careful when disposing of disks, diskettes, or tapes that contain confidential data. Before these media are thrown away or recycled, they must be degaussed, overwritten, or shredded. (Degaussing erases data through demagnetization.) The WIPEDISK program in the Norton Utilities package (available under the PC contract for about $100) destroys all data on a disk by overwriting them.

- When erasing individual files on diskettes or fixed disks, use an overwriting program like WIPEFILE in the Norton Utilities package. These overwriting programs are effective; be careful not to erase needed files.

  It should be noted that programs designed to purge and overwrite individual files (like WIPEFILE) may only overwrite the most recent generation of a file. This would also destroy previous generations of the file if they were physically located in the same disk addresses as the last generation of the file. If the previous generations were located elsewhere on the disk, or if the last generation file is smaller than the previous generations, the previous generations may not be entirely overwritten by the file destruction utility. Recovery of these undestroyed fragments, however, would be extremely difficult and tedious for even the most knowledgeable intruder, and it is unlikely that more than small fragments of the sensitive information could be recovered.)

- If passwords are selected as a control measure (based on the procedural guidance below), make sure passwords are selected and handled as follows:

  - Passwords are at least six characters long
  - Passwords contain at least one alpha and one numeric character
  - Passwords are not composed of names or similar personal types of information
  - Passwords are not shared
  - Passwords are changed at least quarterly
  - Passwords are not written out and left where an unauthorized person could find them
  - Passwords are not incorporated into automated log-on procedures in batch files or application programs (for example, Crosstalk) and they are not defined under function keys.

  Passwords can either be incorporated into applications systems or implemented through add-on circuit boards. While application-based password schemes may prevent casual intruders, they usually do not thwart

the knowledgeable intruder unless special steps are taken (for example, encryption). Knowledgeable intruders may be able to avoid the passwords altogether or may scan application listings to determine the password. For this reason, the more sophisticated hardware-based password schemes are recommended. Cylock, available under the PC contract for about $300, is hardware based.

7.6.3.2 Procedures for Stand-Alone Processing

This part applies to PCs that process in isolation and do not communicate with any other equipment.

CONFIDENTIAL DATA ON REMOVABLE MEDIA ONLY; SINGLE OR SHARED USER PC

Clear the system of confidential information after each confidential processing session. Power off the unit to clear any volatile memory, that is, random access memory (RAM).

CONFIDENTIAL DATA ON NON-REMOVABLE MEDIA; SINGLE OR SHARED USER PC

Keep the computer under lock and key when not in use, that is, keep it in a locked cabinet or a locked room.

If all users of a shared PC have access to all information processed on the PC, establish a formal list of those authorized users (an administrative control). Limit access to those on this authorized list. If this is not the case, users must be protected from each other via either a password scheme or encryption. Encryption software (Datasafe) is available under the PC contract for under $100.

7.6.3.3 Procedures for Communicating PCs

This part applies to PCs that are connected to other equipment such as auto-answer modems, other PCs, or resource servers.

AUTOANSWER MODEM; SINGLE USER OR SHARED

PCs are sometimes used as host systems. An autoanswer modem allows a person to use the system remotely. Keep the computer under lock and key when not in use, that is, keep it in a locked room or a locked cabinet.

Use a password scheme that requires both a traditional user identifier and a password logon process. Under no circumstances should users share passwords.

TERMINAL EMULATION

At times, a PC is used as a terminal device to a large host system. In this situation, security controls are the responsibility of the host system. The host should control access and the extent to which data are sent (uploaded) or received (downloaded).

The PC user needs to make sure he/she adheres to all host-imposed security requirements. In addition, the PC must never store host telephone numbers, logon sequences, or passwords in the PC itself.

LOCAL AREA NETWORKS; SINGLE USER OR SHARED PC

No confidential data may be loaded on to a local area network (LAN) or made available via a LAN unless specifically approved in writing by the Director, OIRM.

7.6.4 Procedures to Preserve High-Level Confidentiality

The EPA has only one type of information in this category - National Security Information (NSI). The amount of NSI possessed by the Agency is extremely small and the need to computerize any of it would be very infrequent.

Because of the small quantity of NSI in the Agency and because NSI involves special security considerations (emanations security and TEMPEST devices), NSI should not be placed on PCs without the express approval of the Director, OIRM.

8. SECURITY FOR WORD PROCESSORS

8.1 INTRODUCTION

This section applies to users of equipment designed primarily for word processing, such as the remaining Lexitrons still in use. Such equipment has little or no programming capability. Under certain circumstances, this section applies to the newer Telex devices (which have been replacing Lexitrons) and to PCs. This section can be used for a Telex or PC if all of the following conditions are met :

- The Telex or PC is used exclusively for word processing
- The Telex or PC does not communicate with other computers
- Confidential documents are never stored on non-removable media like a fixed disk

If the above conditions are not met, the Telex or PC is covered by the Section 7 procedures. (The Telex is a programmable, IBM-compatible microcomputer, making Section 7 applicable when the conditions above are not met.)

In terms of security threats and safeguards, word processors have much in common with PCs. Both are office automation microsystems used by large numbers of EPA employees. In essence, the procedures presented here are a simpler, quicker-to-use version of the PC procedures set forth in Section 7.

The remainder of this section is organized as follows. The next subsection identifies and describes specific threats to information security. Subsections 8.3 and 8.4 specify security measures for maintaining availability and preserving information integrity, respectively. The last subsection specifies security measures for preserving information confidentiality. If more than one security objective applies to the word processor (for example, availability and confidentiality), make sure to review the subsection for each applicable objective.

8.2 THREATS TO SECURITY

8.2.1 Threats to Information Availability

Specific threats to information availability include:

- Hardware Failure: In some cases, word processors are incapable of

being restarted because of hardware failure In addition, sometimes the hardware fails during use for a variety of reasons. The most common problem is a disruption or surge of electrical power, but the failure of almost any internal component can cause the system to crash.

- Accidental Data Destruction: The most common way that information is accidentally destroyed is by users issuing incorrect commands. For example, documents can be inadvertently deleted.

- Sabotage: Information can be deliberately destroyed by malicious individuals. Such destruction can be the result of random vandalism, but it can also be an act by an employee who has been dismissed or disciplined, or an act by an individual who is hostile to the mission of the office.

Two additional threats to availability — theft and damage to media — were discussed in Section 3.

8.2.2 Threats to Information Integrity

Specific threats to information integrity include:

- Deliberate Distortion of Information – Fraud and Sabotage: Data integrity can be damaged by the deliberate actions of system users or other individuals with access to the systems. These actions could be motivated by revenge (for example, by recently disciplined or reprimanded employees) or could be intended to perpetrate or cover up fraudulent activities, mismanagement, or waste.

- Accidental Damage: This occurs when individuals unknowingly modify information or erase pages and documents.

Accidental threats to information integrity overlap with the issues discussed under availability. The distinction is based on whether the distortion is discovered. If so, the distortion would be generally be considered to consist of a loss of information and would therefore be considered to be a availability problem. When the damage remains undetected, decisions may be made or other actions may be taken based upon incorrect information, resulting in a failure of integrity.

8.2.3 Threats to Information Confidentiality

Specific threats to information confidentiality are largely problems of access control. Note that the threats described below apply to confidential information in its various forms, that is, in hard copy, on removable media like diskettes, and on printer ribbons.

- Magnetic media containing confidential information can be accessed by individuals from whom the information should be restricted. If diskettes containing confidential information are not secured, unauthorized individuals can install them on a microsystem and browse their contents.

- Unauthorized individuals could see information on a screen or printout if confidential data are processed in an unsecured area or if printouts are not protected in storage.

- Confidential information can be deciphered from printer ribbons used to print confidential reports.

- Individuals authorized to access confidential information could deliberately share printed reports or magnetic media containing confidential data with unauthorized individuals.

8.3 PROCEDURES TO MAINTAIN AVAILABILITY

8.3.1 Lock-up Media

To avoid theft, store media in a locked cabinet or room.

8.3.2 Write Protection

Whenever possible, write-protect files to avoid accidental destruction.

8.3.3 Isolated Storage

Isolate the critical/high value information on its own storage media. This means dedicating the diskette to the one sensitive document or collection of information.

8.3.4 Backups

In general, the most important step to be taken to protect information availability is to make copies of the information. Backups are performed to provide for easy recovery from a disaster. If information has been backed up and if the backup is safely stored, the information will be recoverable — no matter what happens. Note, however, that information or documents that have been created since the last backup may have been lost and may need to be re-input.

Two backup copies should be made of information or documents of medium-level availability. One of the copies should be a hard copy (paper) version for storage in

the office files. The second copy should be on magnetic media and should be kept in a location other than the original (for example, in the offices of another branch or division).

Two backup copies should also be made of information or documents of high-level availability. The paper copy should be stored as above. The copy on magnetic media, however, should be kept in a physically separate, off-site location.

8.4 PROCEDURES TO PRESERVE INTEGRITY

The security measures needed to ensure integrity represent a mix of those associated with maintaining availability and those associated with preserving confidentiality. Availability and confidentiality are almost opposites; backup copies of information made to enhance availability can aggravate the problem of preventing the disclosure of the information. In a very real sense, however, integrity is the objective in the middle.

Integrity involves elements of the availability objective because if information is corrupted or partially destroyed, intact backup copies are essential. On the other hand, integrity involves elements of the confientiality objective because preventing fraud and sabotage are largely problems of controlling access.

8.4.1 Availability-Related Procedures

Adhere to all procedures described in Section 8.3. This will ensure that backups are created.

8.4.2 Confidentiality-Related Procedures

Adhere to the access control procedures described in Section 8.5.

8.5 PROCEDURES TO PRESERVE CONFIDENTIALITY

8.5.1 Procedures for Medium-Level Confidentiality

EPA organizations with statutory authority for certain types of confidential information may issue security procedures dealing exclusively with a particular type of

information (for example, TSCA or FIFRA CBI). Because of statutory requirements, some of those procedures may be more stringent than those required here. EPA employees must make sure that they also adhere to such organizational standards and procedures.

8.5.1.1 Discourage Traffic

Discourage traffic in the area where the word processor is located when in use. Unauthorized individuals should be kept out of the area so that they cannot view data that might appear on the screen.

8.5.1.2 Printer Ribbons

Printer ribbons used to print confidential documents should be considered confidential as well. Destroy exhausted ribbons so that they cannot be deciphered by an unauthorized individual.

8.5.1.3 Disposal

Be careful when disposing of diskettes or paper containing confidential information. Before the paper is thrown away, it must be shredded or burned. Diskettes must either be degaussed or placed in burn bags. (Degaussing erases information through demagnetization.)

8.5.1.4 Lock-Up Media

Lock-up diskettes and paper copies when not in use in a locked cabinet or a locked room.

8.5.1.5 Clear System

Clear the system of confidential information after each confidential processing session. Power-off the unit to clear any volatile memory, that is, random access memory (RAM).

8.5.2 Procedures for High-Level Confidentiality

The EPA has only one type of information in this category - National Security Information. Procedures for handling and storing this information are contained in the "National Security Information Handbook" issued by OARM. The Handbook also contains procedures governing self-inspection.

9. SECURITY FOR APPLICATION SYSTEM DEVELOPMENT, OPERATIONS AND MAINTENANCE

9.1 INTRODUCTION

The determination of application security requirements and appropriate controls requires three-way communication among the owner, application programmer/ system analyst, and processing installation. Once the owner has determined and communicated the system's sensitivity and security objectives, the owner needs to work with the installation and the application programmer/system analyst to develop the appropriate, cost-effective mix of installation and software-based controls. Once the system has become operational, the installation maintains the installation-oriented controls and the owner authorizes users and makes sure the users and the installation adhere to the security requirements.

Security issues and concerns must be an essential part of the entire software lifecycle (from development to operation to modification). If they are not, the owner runs the risk the application will be underprotected or overprotected. Overprotection wastes resources and underprotection requires that security safeguards be imposed after the fact. Retrofitting security measures on a developed piece of software is both complex and expensive.

This section sets forth security procedures for the application system development and operation process. While this section emphasizes the importance of installation involvement in developing a cost-effective mix of system controls, this section deals with security primarily from an application, rather than installation, perspective. The focus here is on application systems and the responsibilities of ownership. The responsibilities of installations and custodians are set forth in Sections 6 and 7. This section is to be used as follows:

- Application Programmers/System Analysts use these procedures to determine what security measures must be in place to protect the availability, confidentiality, and integrity of sensitive Agency applications.

- Owners develop the security specifications and the tests needed for application certification based on the procedures presented here and based on dialogue with the application developers and processing installation.

Owners then make sure the operational application is protected on an ongoing basis using the procedures presented here.

The remainder of this section is organized as follows. The next subsection catalogs and describes the basic application development controls that can be used to achieve the three security objectives. Subsection 9.3 introduces the concept of the software lifecycle and explains how to address, build in, and maintain security controls at the various life cycle stages.

The overall structure and content of this section is based in large part on Federal Information Processing Standards Publication (FIPS PUB) 73, entitled "Guidelines for Security of Computer Applications." FIPS PUB 73 is extremely helpful and application developers may wish to consult it for more detailed information on selected topics. A copy is available in the EPA Headquarters library or through the National Technical Information Service. To a lesser extent, this section is also based on the "Management Guide to the Protection of Information Resources" issued by the National Institute of Standards and Technology.

9.2 BASIC DEVELOPMENT CONTROLS

This subsection introduces six basic development controls to be used to meet the security objectives of availability, integrity, and confidentiality. The six controls, which are explained in detail below, are as follows:

- Data Validation
- User Identity Verification
- Authorization
- Journalling or Logging
- Variance Detection
- Encryption

Table 9-1 shows the security objective (or objectives) addressed by each of these basic controls. Note that most controls preserve confidentiality and integrity rather than maintain availability. This is because continued availability is often achieved through administrative/procedural safeguards such as backup routines and contingency planning.

TABLE 9-1

BASIC CONTROLS AND THE OBJECTIVES THEY ADDRESS

	Objectives		
Control	**Availability**	**Integrity**	**Confidentiality**
• Data Validtion		X	
• User Identity Verification	X	X	X
• Authorization	X	X	X
• Journalling/ Logging	X	X	X
• Variance Detection		X	X
• Encryption		X	X

It should be noted that some of these controls may be partially implemented by the operating system, the hardware, or the management of the processing installation. Such joint implementation results because the boundaries between the application and operating systems or between hardware and software are sometimes fuzzy.

9.2.1 Data Validation

Data validation involves checking data to make sure they are accurate, complete, and consistent. This checking or examination should occur both during entry and during processing. In addition, input data elements should be compared with one another to ensure consistency and reasonableness.

Techniques for validating data during entry include:

- Examining fields for various characteristics, including proper format, values within certain bounds, and check digits.
- Maintaining control totals, record/transaction counts and batch number checks for groups of records or transactions.

Techniques for validating data during processing include:

- Incorporating dummy records into a data base and doing test transactions against these records during normal processing of the application to evaluate processing accuracy.
- Tracing specially marked transactions through the processing cycle to determine if processing was correct.
- Sampling methods where certain data are selected for close examination to determine their validity.

Techniques for ensuring consistency and reasonableness include:

- Comparing one field against another for a certain relationship, for example, one field with a value less than half of another field.
- Evaluating the current record against the previous record.

9.2.2 User Identity Verification

User identity verification involves establishing a means to control access to the application by requiring each individual to prove who he/she is. The basic access

control methods include: (1) passwords, (2) objects like magnetic cards or keys, and (3) personal characteristics such as signatures or voiceprints.

User identification based on personal characteristics like signature is prohibitively expensive. For most on-line applications, the most practical technique is a password scheme.

There are two predominant types of passwords: (1) Host-level passwords, and (2) information access passwords. Host-level passwords are those used when first logging-on to the computer system, for example, VAX, Prime, or IBM mainframe. A host-level password verifies the identity of the user before the user is allowed to do anything on the system.

An information access or "second level" password is used to protect individual files or data sets resident on the computer system. Information access passwords are entered when the logged-on user requests access to a password-protected file or data set. Information access passwords can be either unique like host-level passwords or shared by multiple users needing access to common data. Unique information access passwords require access control software apart from the host-level log-on process.

Host-level passwords are administered by the processing installation, as described in Section 6. NDPD (which operates NCC and WIC and supports other sites) does not advocate the use of information access passwords. Instead, the NCC makes Resource Access Control Facility (RACF) available to application owners. RACF bases information access on user identification; Prime and VAX have similar schemes based upon access control lists (ACL).

Any contemplated use of information access passwords at an NDPD managed or supported facility must be discussed with the Security Officer for that facility. If information access passwords are selected as a control measure, make sure of the following:

- Passwords of at least six characters in length can be accepted
- Passwords must contain at least one alpha and one numeric character
- Passwords can be deleted or changed in a straightforward, but controlled fashion.

9.2.3 Authorization

For automated applications, some users may only be authorized to perform certain functions or to use certain data files. If there are many users of a sophisticated application that has many data files, confidentiality and integrity will be preserved if users are only allowed access to needed functions and files. A basic authorization scheme can be enforced if the application has different interfaces for different purposes, for example, for data entry or for report generation.

While the security literature describes many different types of authorization schemes, they all have three essential features. They control: (1) who will have access, (2) what modes of access they will have, and (3) which objects or resources they will be allowed to access. The "who" component includes both users and terminals. Modes of access usually include read-only access, read/write access, and the like. Objects or resources typically include:

- Data objects like files, record types, and libraries
- Executable objects like commands or programs
- Devices like printers or various storage media such as tapes or disks.

Any authorization scheme that is selected should have two basic properties. First, it should operate under the principle of least privilege where users should be limited to only what they need to do. Second, the scheme should be flexible enough to allow for changes in authorization in a straightforward, yet controlled way.

9.2.4 Journalling or Logging

Journalling or logging involves recording particular events as they occur during data entry or processing. Journalling provides an audit trail for tracking down errors or security violations. Journalling provides a basis for establishing accountability, that is, a basis for holding individuals responsible for their activities. It also may aid in recovering from a processing mishap or disaster.

While it is possible to journal every event and transaction, this is typically impractical and not cost-effective. In selecting what to log, owners and system developers should focus on the type of information and security objectives involved. Clearly a financial system that disburses funds must keep track of who makes each credit and

debit transaction, exactly when each transaction was made, and similar events. In an application where integrity is not as crucial, associating each transaction with a user is probably unnecessary.

Any journalling activity typically falls into one or more of the following categories:

- Logging the nature of the event (for example, system usage like log-ons, input/output like opening a file, or updates like file changes).
- Logging the identity of those associated with the event, including users, devices, or files.
- Logging characteristics of the event such as time, date, or number of data entry errors.

9.2.5 Variance Detection

As the term implies, variance detection is concerned with identifying departures from the norm that are deemed to be of significance. Variance detection may either augment an authorization scheme or be used instead of authorization when authorization is impractical.

Variance detection can be accomplished through:

- Review and analysis of the results of the journalling or logging process
- External methods such as audits or surprise visits
- Dynamic monitoring, which involves real-time detection of certain trigger events. For example, an application designed to electronically transmit funds only at certain times could be programmed to warn the console operator if transfer is attempted at some other time. As a second example, a system can automatically count the number of attempts made to gain access through password guesses before it ends the log-in session.

9.2.6 Encryption

Encryption involves scrambling or encoding information so that it is of no use even if it is obtained by unauthorized individuals. Encryption is the primary means of protecting data during communication. The decision whether or not to encrypt data during communication would depend on the communication configuration. If confidential data are being transmitted over a dedicated line, encryption may be unnecessary unless line tapping is a serious threat. If the data are traveling over a network

where many unauthorized users could potentially intercept the information, encryption may be effective.

Information stored off-line in tapes or other media may also be encrypted to prevent it from being read if it is stolen. In most instances, however, physical security measures (such as keeping the media under lock and key) are easier to implement and are adequate.

The encryption of on-line data files will be cumbersome unless the operating system and hardware have certain supporting capabilities. In most instances, a password protection scheme should probably be sufficient. In instances where it is deemed necessary to supplement the passwords with encryption, choose a processing location like the NCC where the supporting hardware and operating system features are already in place.

9.3 CONTROLS AND THE SOFTWARE LIFECYCLE

9.3.1 The Software Lifecycle

The only way to ensure that the kind of controls described in Section 9.2 are correctly implemented is to make them an explicit part of the software development process. The three-volume "EPA System Design and Development Guidance" issued by OIRM describes the software design and development process at EPA and includes general references to security at appropriate points. The "Operations and Maintenance Manual," also issued by OIRM, completes the guidance for managing the software lifecycle by addressing the day-to-day performance of system operations and maintenance activities. It also includes general references to security at appropriate points. The purpose of this section is to describe more specifically how to incorporate security controls into the lifecycle.

The "EPA System Design and Development Guidance" and the "Operations and Maintenance Manual" define four basic lifecycle phases:

Phase 1: Mission Need Analysis

Phase 2: Preliminary Design and Option Analysis

Phase 3: System Design, Development, and Implementation, including system testing and evaluation

Phase 4: Operations and Maintenance

At a minimum, application development and operation need to include security specifications, security design reviews, system tests of security controls, and ongoing system monitoring to ensure controls are implemented. Table 9-2 presents the relationship between these requirements, the EPA lifecycle, and the participants or roles associated with the lifecycle.

The process begins with the owner's determination of sensitivity and relevant security objectives. The next step is to develop control requirements based on Section 9.2. Determining a cost-effective mix of adequate controls depends on the owner understanding why the application is sensitive (that is, relevant security objectives and degree of sensitivity) and the types of controls the processing installation can provide to address that sensitivity.

If the availability objective is relevant to the application, the owner needs to determine backup and availability requirements and communicate them to the installation. The owner then needs to make sure the installation can satisfy any special requirements, such as more frequent backup than is typical or the need for continuous availability (that is, downtime of more than just a few hours would be unacceptable).

As the development process proceeds, the owner creates the security information needed for the Application Certification Worksheet. Please see Appendix B.

The development process ends with the application being placed into use or production. This is a formal milestone that clearly separates the developmental version of the system from the operational version. At this point, key security responsibilities transfer to the installation; the required installation controls are specified in Section 6. Once the system is ready to use, the owner needs to make decisions about who can access the system and what kind of access they will have (for example, read-only access). The responsibilities of ownership do not end at this point, however. On a continuing basis, the owner needs to make sure the application is protected and that the users and installation adhere to security requirements.

In the middle of the development process, the focus is on security design and testing. These activities are the subject of Subsection 9.3.2 below.

TABLE 9-2

SECURITY AND THE SOFTWARE LIFECYCLE

Lifecycle Phase	Security Activity	Role/ Participant
Mission Need Analysis	Identification of Security Needs and Considerations	Owner
Preliminary Design and Options Analysis	Determine Security Requirements and Specifications	Owner with Application Programmer/ System Analyst and Mini/ Mainframe Computer Security Officer
System Design, Development, and Implementation	Design Controls; Conduct Design Review; Test and Review Security Controls; Determine Backup and Availability Requirements	Application Programmer/System Analyst with Owner Conducting Reviews; Owner Determines Back-up and Availability Needs
Operations and Maintenance	Maintain/Alter Security Controls as needed; Authorize Users; Monitor Users/Installation for Compliance with Security Requirements	Owner with Application Programmer as needed and Mini/ Mainframe Computer Security Officer Implementing Installation-Based Controls

9.3.2 Implementing Controls: Building Security into the Development Phase

9.3.2.1 Designing for Security

This is the stage when decisions about how to implement the basic development controls must be made. Security considerations should be an integral part of the overall design effort because security opportunities missed now will be difficult to recapture later. In designing the necessary basic controls, adhere to the following overall procedures:

- Restrict user interfaces to the functions and files users need to access. Unnecessary flexibility greatly complicates security. Limit the number of unsuccessful attempts to access an application or file. It should be noted that certain processing facilities have made access control features readily available. For example, Resource Access Control Facility (RACF) is available on the NCC IBM mainframe and on the logical mainframes. RACF can be used to protect data sets from unauthorized users or from deletion. The NCC and other installations also limit the number of consecutive password failures before a user is blocked from the system. See the "NDPD Operational Policies Manual" for more information.

- Design user interfaces that are easy to understand. This reduces user errors and the potential for data corruption. Specific engineering tasks can include intelligible system and error messages and on-line help functions.

- If the application will be used continuously and has significant storage requirements, consider dedicating a micro or minicomputer to the application. The choice of hardware environment involves many other factors, including needed physical security, access controls, and logging/auditing capability. Dedicated hardware, such as a micro or minicomputer, can make it easier to protect software and data. In many circumstances a mainframe environment may be more appropriate. This is why three-way communication among the owner, application developer, and installation is important.

- Isolate the code that is critical to security. If possible, create separate modules for the security controls, which facilitates both protection and audit. Consider using automated controls to protect these modules. These include: (1) checksums on the object code to detect unauthorized changes, (2) hardware protection states or domains to protect code, and (3) placin g critical code in a fixed area of memory so that read-only memory can be used.

- Design the system so that it is auditable, that is, so that it is relatively easy to confirm that the system is functioning as it was intended to function. Systems that are not designed for auditability are harder to test and evaluate.

- If availability is important, design the system so that recovery from minor

problems or major disruptions is facilitated. For example, if a computer at another site has been designated as a backup, make sure the system is readily transportable to the alternative environment.

9.3.2.2 Programming for Security

Programming practices can have three impacts on security. First, errors in programming security controls (such as journalling or logging) can limit or cancel the effectiveness of the control. Second, programming errors in the non-security-related portions of the code can greatly affect data reliability and accuracy. Finally, unauthorized additions or changes to the code by programmers can result in fraud or abuse.

During the programming stage, adhere to the following practices:

- Have each section of the code peer-reviewed as it is completed. The review should focus on the efficiency, maintainability, and correctness of the code.
- Have the program library:
  - Limit access to program modules to authorized individuals
  - Record all accesses to program modules
  - Store previous versions of a module so that comparisons with the present version can be made.
- Document all security-related portions or modules of code. Security-related code is code that implements basic controls, code that accesses sensitive data, or code that processes sensitive data. Once the documentation is developed, it also needs to be protected so that the integrity or confidentiality of the system are not compromised.

9.3.2.3 Testing and Evaluating Software

The last thing the application developer needs to do is to test the software to make sure it meets the security requirements. Effective testing begins with the development of a test plan, which describes what will be tested with what methods. For effective security testing, particular emphasis should be placed on how the application handles unusual, unlikely, and illegal events.

The test plan should include both static evaluation and dynamic evaluation. For

static evaluation, the following techniques are recommended:

- Code review by an independent party
- Source code analyzers to provide details about selected characteristics of the source program
- Penetration analysis to determine whether a determined individual could bypass controls.

Dynamic evaluation is concerned with testing the operation of portions of the program with dummy data and comparing the results with the expected results. To aid in the evaluation process, the following techniques are recommended:

- Program analyzers to collect operating data about the executing program, for example, the number of times a particular data file is accessed
- Comparative analysis, which involves testing the new system for known flaws in similar existing systems.

If disclosing confidential information is a security concern, care should be taken when granting individuals testing the software access to "live" data from the operational environment.

9.3.3 Operating and Maintaining Controls

Security considerations do not cease once the application becomes operational. Even the best conceived and developed controls need to be managed on a continuing basis. In operating and maintaining security safeguards, adhere to the following procedures:

- As the system becomes operational, the owner needs to make decisions about who can access the system and what kind of access they will have (for example, read-only access). The responsibilities of ownership do not end at this point, however. On an ongoing basis, the owner needs to make sure that the application is protected and that users and the installation adhere to security requirements. At a very minimum, the application must be re-certified every three years (see Appendix B).
- Mechanisms for ensuring ongoing compliance can vary from system to system. If, for example, journalling/logging or variance detection are important controls, the owner can request that the installation produce standard reports. If frequent backup is essential, the owner can simulate a disaster by requesting that certain files be restored within a specified time period. Or, the owner may structure an internal control review or related study as part of the Agency's internal control review process to

gauge user and installation compliance with security requirements.

In monitoring compliance, it is not expected that the owner will have a detailed technical understanding of how all his/her security controls work (for example, how an encryption algorithm operates or how variance detection code operates), but rather that he/she will take the steps needed to be confident that the system is adequately protected.

- Maintenance programmers are subject to the same procedures as system development programmers for programming, testing, and evaluating software (see Section 9.3.2). In addition, if disclosing confidential information is a security concern, care should be taken when granting maintenance programmers access to "live" confidential systems for problem identification or testing purposes.

10. SECURITY FOR PAPER AND MICROFORM RECORDS

10.1 INTRODUCTION

The purpose of this section is to describe the security measures that need to be taken to ensure adequate protection of collections of paper and microform (that is, microfiche and microfilm) records. The focus here is not on normal desk or office files, but rather on significant quantities of records that constitute manual information systems.

This section is to be used as follows:

- Owners develop the security requirements for the information collection based on the procedures presented here.
- Records Management Officers assign responsibility for the physical custody of the records and make sure that custodians are properly implementing these procedures.
- Custodians are responsible for making sure the necessary security controls are in place.

The remainder of this section is organized as follows. The next subsection explains the relationship between this section and other Agency security procedures, for example, the "TSCA CBI Manual." Subsection 10.3 catalogs and describes specific threats to the security of manual information systems. The last three subsections set forth security measures for ensuring the availability, integrity, and confidentiality of record systems. If more than one objective applies to the record system (for example, availability and confidentiality), make sure to review the subsection for each applicable objective.

10.2 RELATIONSHIP TO OTHER PROCEDURES

Over the years, the EPA has developed several sets of procedures governing specific types of sensitive information. The great majority of these existing procedures deal with some type of confidential information, especially CBI. These procedures are typically issued by EPA organizations with statutory authority for the information (for example, the Office of Pesticides and Toxic Substances for TSCA

or FIFRA CBI). EPA employees must make sure they adhere to all of these organizational standards and procedures, as well as to the procedures presented here.

The scope and nature of these other, type-of-information procedures is as follows:

- The Office of Administration and Resources Management has issued procedures governing National Security Information (in the "National Security Information Handbook") and Privacy Act data. The NSI handbook also contains self-inspection procedures for organizations dealing with National Security Information.
- The Office of Pesticides and Toxic Substances has developed manuals governing both TSCA and FIFRA CBI.
- The Office of Solid Waste and Emergency Response has issued procedures concerning RCRA CBI.
- The Office of Enforcement and Compliance Monitoring has established enforcement docket security procedures for handling and disposing of docket reports.
- Within the Office of Air and Radiation, the Office of Mobile Sources has procedures for the handling of proprietary data received from auto manufacturers and the Office of Air Quality Planning and Standards (Emission Standards and Engineering Division) has procedures for safeguarding the CBI it receives.
- The Office of the Inspector General Manual contains sections dealing with confidential information obtained during the course of investigations and audits.
- The Office of Water has developed procedures related to trade secret data obtained under Section 308 of the Clean Water Act.

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

10.3 THREATS TO MANUAL INFORMATION SYSTEMS

10.3.1 Threats to Availability

Specific threats to record availability include:

- Theft: Paper and microform records are small, light, and easily moved.

- Accidental Destruction of Records: A record may be accidentally destroyed or lost through an act of nature (such as a flood or fire) or through human error (such as inadvertently throwing it away).

- Deliberate Destruction of Records: Records can be deliberately destroyed by malicious individuals. Such destruction can be the result of random vandalism, but it can also be an act by an employee who has been dismissed, disciplined, or is hostile to the mission of the office.

10.3.2 Threats to Integrity

Specific threats to record integrity include:

- Accidental Damage: This occurs when individuals inadvertently and unknowingly change records. While this is a common threat to automated information systems, it is less prevalent for manual systems. It would occur, for example, if a system of records became jumbled. If the disorganization went undetected, decisions could be made based on information that seemed complete, but was not because crucial information had been misfiled elsewhere.

- Deliberate Distortion of Records Through Fraud and Sabotage: The integrity of records can be damaged by the deliberate actions of individuals with access to the records. These actions could be motivated by revenge (for example, by recently disciplined or reprimanded employees) or could be intended to perpetrate or cover up fraudulent activities, mismanagement, or waste.

10.3.3 Threats to Confidentiality

Threats to confidentiality are largely problems of access control. Specific threats to record confidentiality include:

- Unauthorized Disclosure: If rooms or cabinets housing confidential records are not secure, unauthorized individuals can open them and review the records. Unauthorized disclosure can also occur if authorized individuals deliberately share confidential records with unauthorized individuals.

- Typewriter and Printer Ribbons: Confidential information can be deciphered from typewriter and printer ribbons that have been used to produce confidential reports.

10.4 PROCEDURES TO MAINTAIN AVAILABILITY

10.4.1 Procedures for Medium-Level Availability

10.4.1.1 Environmental Controls

To avoid water damage, do not store the records directly beneath sprinkler heads or water pipes. Do not locate the records near boiler rooms or water heaters.

10.4.1.2 Access Control List

The information owner must establish for the custodian a list of individuals who are allowed access to the records. On a quarterly basis, the owner should review the list to update it with employee additions or deletions.

10.4.1.3 Document Control and Tracking

To prevent the loss of records, establish a document control and tracking system. This system may be automated or manual. In either the case, the system must include:

- A unique identifier, the Document Control Number (DCN), for each document in the collection of records.
- A cradle-to-grave tracking capability which follows a record from the time it is received or written until it is destroyed or transferred elsewhere. For a manual system, the worksheets shown as Exhibits 10-1 and 10-2 can be used. Exhibit 10-1 is an inventory of all records in the collection. Exhibit 10-2 is a sign-out log indicating who has which records. Automated tracking systems should capture the same information shown in the exhibits, that is:
  - Date record created or received
  - DCN
  - Dates record checked out and returned
  - Identity of who has a checked out record
  - The disposition of a record, that is, transfer or destruction

10.4.1.4 Backup Copy

Maintain a second copy of the records at an off-site storage location. In the event of a major disaster that destroys the original set of records, this second set will prove invaluable. The backup copy may be in several different forms, including microfiche,

EXHIBIT 10-1

INVENTORY

Date Received	DCN	No. of Pages	Document Originator	Disposition

EXHIBIT 10-2

SIGN-OUT LOG

Date Checked Out	DCN	User Information		Date Checked In
		User Name	EPA ID Number	

paper, or word processing diskettes.

10.4.2 Procedures for High-Level Availability

This part applies to all record collections that must be available continuously or within one day and/or collections that are of very high value. All procedures set forth in Subsection 10.4.1 also apply here. In addition, the procedures described below will be followed.

10.4.2.1 Fire Protection

Store the records in a fireproof file cabinet.

10.4.2.2 More Accessible Backup Copy

For critical collections, make sure the second copy that is being stored at an off-site location can be retrieved within a few hours. Storage locations that require one to two days notice to retrieve records are of limited usefulness.

10.5 PROCEDURES TO MAINTAIN INTEGRITY

The security measures needed to ensure integrity represent a mix of those associated with maintaining availability and those associated with preserving confidentiality. As was noted earlier, copies of records made to enhance availability can aggravate the problem of preventing the disclosure of information stored in the record collection. In a very real sense, integrity is the objective in the middle.

Integrity involves elements of the availability objective because if information is altered or partially destroyed, an intact backup copy is essential. On the other hand, integrity involves elements of the confidentiality objective because preventing fraud and sabotage are largely problems of controlling access.

10.5.1 Procedures for Medium-Level Integrity

10.5.1.1 Availability-Related Procedures

Adhere to all procedures described in Section 10.4.1.

10.5.1.2 Confidentiality-Related Procedures

Make sure the records are kept in a locked cabinet or a locked room. Use the lock

whenever the records are not in use, not just at night. If the lock is a combination lock, change the combination at least annually or whenever there is a change in who is allowed access to the records.

10.5.2 Procedures for High-Level Integrity

All procedures set forth in Section 10.5.1 above also apply here. In addition, store the records in a fireproof cabinet or container.

10.6 PROCEDURES TO PRESERVE CONFIDENTIALITY

Preserving confidentiality involves controlling access to information and records. Access controls for manual information systems are of two types: (1) physical, such as door locks, and (2) administrative, such as lists which specify who is allowed access to the records.

10.6.1 Procedures for Medium-Level Confidentiality

10.6.1.1 Access Control List

The information owner must establish for the custodian a list of individuals who are allowed access to the records. On a monthly basis, the owner should review the list to update it with any additions or deletions.

10.6.1.2 Document Control and Tracking

To maintain accountability and to further control access, establish a document control and tracking system. This system may be automated or manual. Develop and maintain the system in accordance with the procedures described in Section 10.4.1.3.

10.6.1.3 Lock Up Records

Make sure the records are kept in a locked cabinet or a locked room. Use the lock whenever the records are not in use, not just at night. If the lock is a combination lock, change the combination at least annually or whenever there is a change in who is allowed access to the records.

10.6.1.4 Photocopies

A lack of photocopying controls can defeat strong access controls in other areas. It

does little good to lock everything up and log each document in and out if the person using the document is allowed to make copies at will.

Only the owner or custodian should be allowed to make photocopies. Photocopying by all others should be prohibited. All photocopies must be entered into the document control and tracking system under their own DCNs.

10.6.1.5 Disposal

All confidential paper documents must be shredded or burned before being thrown away. Place discarded microfiche or microfilm into burn bags for proper disposal.

10.6.1.6 Typewriter and Printer Ribbons

Ribbons used to produce confidential documents should be considered confidential as well. Place exhausted ribbons in burn bags so that they cannot be deciphered by an unauthorized individual.

10.6.2 Procedures for High-Level Confidentiality

The EPA has only one type of information in this category - National Security Information (NSI). Procedures for handling and storing NSI are contained in the "NSI Handbook" issued by OARM.

APPENDIX A
INFORMATION SECURITY *

1. PURPOSE. This document establishes a comprehensive, Agency-wide security program to safeguard Agency information resources. This document sets forth the Agency's information security policy for both manual and automated systems and assigns individual and organizational responsibilities for implementing and administering the program.

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

3. BACKGROUND

a. Information is an Agency asset, just as property, funds and personnel are Agency assets. The EPA is highly dependent upon its information resources to carry out program and administrative functions in a timely, efficient and accountable manner.

b. The EPA relies on its information collection authority under various enabling statutes to fulfill effectively its environmental missions. The willingness of the regulated community and State and local agencies to supply requested information in a cooperative and timely fashion depends on their confidence that the information will be adequately protected.

c. The Agency's information resources are exposed to potential loss and misuse from a variety of accidental and deliberate causes. This potential loss and misuse can take the form of destruction, disclosure, alteration, delay or undesired manipulation. Moreover, the Agency can be subject to acute embarrassment and litigation if certain business or personal information is inadvertently or maliciously disclosed.

d. As a result, it is essential that an overall program be established to preserve and adequately protect the Agency's information resources. At the same time, it is equally essential that the program not unnecessarily restrict information sharing with other Federal agencies, universities, the

*** Source: EPA Information Resources Management Policy Manual, Chapter 8.**

public and State and local environmental authorities. Such information sharing has historically played a vital role in the overall fulfillment of the Agency environmental mission.

e. The management, control and responsibility for information resources within EPA are decentralized. Consequently, the management and responsibility for information security are also decentralized. An important example of this is the expanding use of personal computers, networking, distributed data bases and telecommunications. These trends place new responsibilities on office managers, research personnel and others not previously considered information processing professionals. The "computer center" cannot be relied upon to protect Agency operations. Controls must be implemented and maintained where they are most effective.

f. In determining responsibilities for information security, it is useful to define a framework of owner/custodian/user. Owners are those who create or maintain information. Custodians are typically suppliers of information services who possess, store, process and transmit the information. These roles are often not discrete; the owner is often the principal custodian and user of the information.

4. AUTHORITIES

a. OMB Circular A-130, Management of Federal Information Resources.

5. POLICY. It is EPA policy to protect adequately sensitive information and sensitive applications, maintained in any medium (e.g., paper, computerized data bases, etc.), from improper use, alteration or disclosure, whether accidental or deliberate. Information and applications will be protected to the extent required by applicable law and regulation in accordance with the degree of their sensitivity in order to ensure the cost-effectiveness of the security program.

a. Information security measures will be applied judiciously to ensure that automated systems operate effectively and accurately and to ensure the continuity of operation of automated information systems and facilities that support critical agency functions.

b. As required by OMB Circular No. A-130, all automated installations will undergo a periodic risk analysis to ensure that appropriate, cost-effective safeguards are in place. This risk analysis will be conducted on new installations, on existing installations undergoing significant change and on existing installations at least every five years.

c. Appropriate administrative, physical, and technical safeguards shall be incorporated into all new ADP application systems (including PC-based applications) and major modifications to existing systems.

d. As required by OMB A-130, all new applications will undergo a control review leading to formal certification. Existing sensitive applications will be recertified every three years.

e. Access to sensitive personnel information and employment applications will be limited to appropriate personnel in accordance with procedures established by the Office of Personnel Management and monitored by the EPA Office of the Inspector General.

f. Appropriate ADP security requirements will be incorporated into specifications for the acquisition of ADP related services and products.

g. An information security awareness and training program will be established so that all Agency and contractor personnel are aware of their information security responsibilities.

h. Information security must be a major factor in evaluating the use of microcomputers. Microcomputer systems software is typically rudimentary and affords little or no protection to information and programs. Consequently, networked microcomputers, the ability to download data from larger, protected computers onto microcomputers and microcomputer data processing, generally present problems in information security (for example, problems of access control or control over the dissemination of information). All EPA employees and managers must be aware of the information security implications of storing and processing sensitive information on microcomputers, whether networked or stand-alone.

i. Therefore, it is EPA policy to discourage the use of microcomputers for storing or processing sensitive information, unless cognizant EPA employees and managers have made sure that adequate information security measures are in use. If adequate information security cannot be maintained, an alternative system configuration must be used.

j. Information security violations will be promptly reported to appropriate officials, including the Inspector General.

6. RESPONSIBILITIES

a. The Office of Information Resources Management is responsible for:

(1) Developing and issuing an information security policy in accordance with all applicable Federal laws, regulations, and executive orders.

(2) Ensuring that all Agency organizational units are in compliance with the information security program.

(3) Establishing training criteria and coordinating the development of an information security training and awareness program.

(4) Providing guidance on selecting and implementing safeguards.

(5) Participating as it deems appropriate, in management and internal control reviews conducted by the Office of the Comptroller to ensure compliance with the information security program.

b. Each "Primary Organization Head" (defined by EPA Order 1000.24 as the Deputy Administrator, Assistant Administrators, Regional Administrators, the Inspector General and the General Counsel) is responsible for:

(1) Ensuring that sensitive information and applications within the organization are adequately protected.

(2) Establishing an organization-wide program for information security consistent with organizational mission and Agency policy, including assigning responsibility for the security of each installation to a management official(s) knowledgeable in information technology and security.

(3) Assure annually the Assistant Administrator for Administration and Resources Management that organizational information resources are adequately protected. This will be done as part of the internal control review process required under OMB Circular No. A-123 (revised) and implemented under EPA Order 1000.24.

(4) Making sure that all automated installations within the organization undergo a periodic "risk analysis" to ensure that appropriate, cost-effective safeguards are in place.

(5) Ensuring the continuity of operations of automated information systems and facilities that support critical functions.

(6) Making sure that appropriate safeguards are incorporated into all new organizational application systems and major modifications to existing systems, that all new organizational applications undergo an information security review leading to formal certification and that existing sensitive applications are recertified every three years.

(7) Making sure that Federal employees and contractor personnel understand their security responsibilities and that organizational security regulations are properly distributed.

(8) Making sure that all organizational procurements of ADP equipment, software and services incorporate adequate security provisions.

c. The Director, Facilities Management and Services Division, is responsible for:

(1) Establishing and implementing physical security standards, guidelines and procedures in accordance with EPA information security policy.

(2) Establishing and implementing standards and procedures for National Security Information in accordance with EPA information security policy and all applicable Federal laws, regulations and executive orders.

d. The Procurement and Contracts Management Division and the Grants Administration Division are responsible for:

(1) Ensuring that Agency grant and contract policies, solicitations and award documents contain provisions concerning the information security responsibilities of contractors and grantees that have been promulgated by OIRM.

(2) Establishing procedures to ensure that contractors and grantees are in compliance with their information security responsibilities. Project Officers are responsible for ensuring contractor compliance with security requirements on individual contracts. Violations shall be reported to the contracting officer, Inspector General and appropriate OIRM official. Specific violations involving National Security Information shall be reported to the Director, FMSD and the Contracting Officer.

e. The Office of the Inspector General is responsible for:

(1) Establishing and implementing personnel security standards, guidelines and procedures in accordance with EPA information security policy and all applicable Federal laws and regulations.

(2) Conducting or arranging investigations of known or suspected personnel security violations as it deems appropriate.

f. The Office of the Comptroller is responsible for:

(1) Allowing OIRM to review written internal control reports so that OIRM is aware of the status of information security weaknesses.

g. Each EPA Manager and Supervisor is responsible for:

(1) Making sure their employees are knowledgeable of their information security responsibilities.

(2) Ensuring that their employees adhere to the organizational information security program established by the applicable Primary Organization Head.

h. Each EPA Employee, Contractor and Grantee is responsible for:

(1) Complying fully with his/her information security responsibilities.

(2) Limiting his/her access only to information and systems he/she is authorized to see and use.

(3) Adhering to all Agency and organizational information security policies, standards and procedures.

(4) Reporting information security violations to appropriate officials. Violations involving National Security Information shall also be reported to the Director, FMSD.

7. DEFINITIONS.

a. "Applications Security" means the set of controls that makes an information system perform in an accurate and reliable manner, only those functions it was designed to perform. The set of controls includes the following: programming, access, source document, input data, processing storage, output and audit trail.

b. "Confidential Business Information" includes trade secrets, proprietary, commercial/financial information, and other information that is afforded protection from disclosure under certain circumstances as described in statutes administered by the Agency. Business information is entitled to confidential treatment if: (1) business asserts a confidentiality claim, (2) business shows it has taken its own measures to protect the information, (3) the information is not publicly available or (4) disclosure is not required by statute and the disclosure would either cause competitive harm or impair the Agency's ability to obtain necessary information in the future.

c. "Information" means any communication or reception of knowledge such as facts, data or opinions, including numerical, graphic, or narrative forms, whether oral or maintained in any medium, including computerized data bases (e.g., floppy disk and hard disk), papers, microform (microfiche or microfilm), or magnetic tape.

d. "Information Security" encompasses three different "types" of security: applications security, installation security and personnel security. In total, information security involves the precautions taken to protect the confidentiality integrity and availability of information.

e. "Information System" means the organized collection, processing, transmission and dissemination of information in accordance with defined procedures, whether automated or manual.

f. "Installation" means the physical location of one or more information systems, whether automated or manual. An automated installation consists of one or more computer or office automation systems including related peripheral and storage units, central processing units, telecommunications and operating and support system software. Automated installations may range in size from large centralized computer centers to stand-alone personal computers.

g. "Installation Security" includes the use of locks, badges and similar measures to control access to the installation and the measures required

for the protection of the structure housing the installation from accident, fire and environmental hazards. In addition to the above physical security measures, installation security also involves ensuring continuity of operations through disaster planning.

h. "National Security Information" means information that is classified as Top Secret, Secret, or Confidential under Executive Order 12356 or predecessor orders.

i. "Personnel Security" involves making a determination of an applicant's or employee's loyalty and trustworthiness by ensuring that personnel investigations are completed commensurate with position sensitivity definitions according to the degree and level of access to sensitive information.

j. "Privacy" is the right of an individual to control the collection, storage and dissemination of information about himself/herself to avoid the potential for substantial harm, embarrassment, inconvenience or unfairness.

k. "Risk Analysis" is a means of measuring and assessing the relative vulnerabilities and threats to a collection of sensitive data and the people, systems and installations involved in storing and processing that data. Its purpose is to determine how security measures can be effectively applied to minimize potential loss. Risk analyses may vary from an informal, quantitative review of a microcomputer installation to a formal, fully quantified review of a major computer center.

l. "Sensitive Information" means information that requires protection due to the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration or destruction of the information. For the purposes of this program, information is categorized as being either sensitive or not sensitive. Because sensitivity is a matter of degree, certain sensitive information is further defined as being "highly" sensitive.

<u>Highly Sensitive</u>: This is information whose loss would seriously affect the Agency's ability to function, threaten the national security or jeopardize human life and welfare. Specifically, information of this type includes National Security Information, information critical to the performance of a primary Agency mission, information that is life critical and financial information related to check issuance, funds transfer and similar asset accounting/control functions.

<u>Other Sensitive</u>: This is information whose loss would acutely embarrass the Agency, subject the Agency to litigation or impair the long-run ability of the Agency to fulfill its mission. Information of this

type includes Privacy Act information, Confidential Business Information, enforcement confidential information, information that the Freedom of Information Act exempts from disclosure, budgetary data prior to release by OMB and information of high value to the Agency or a particular organization (see below).

The sensitivity if any, of all other information, shall be determined by the organizational owner of the information. While a precise set of criteria for determining the sensitivity of this other information cannot be provided, the cost of replacing the information and the problems that would result from doing without the information are primary factors to consider in determining sensitivity.

m. "Sensitive Applications (or Systems)" are applications which process highly sensitive or sensitive information or are applications that require protection because of the loss or harm which could result from the improper operation or deliberate manipulation of the application itself. Automated decision-making applications are highly sensitive if the wrong automated decision could cause serious loss.

8. PROCEDURES AND GUIDELINES. Standards, procedures and guidelines for the Agency information security program will be identified and issued under separate cover in the "Information Security Manual." This manual will identify and reference, as appropriate existing procedures in the information security area, such as the "Privacy Act Manual," the "National Security Information Security Handbook," and Confidential Business Information manuals like the TSCA Security Manual.

9. PENALTIES FOR UNAUTHORIZED DISCLOSURE OF INFORMATION.

a. EPA employees are subject to appropriate penalties if they knowingly, willfully or negligently disclose sensitive information to unauthorized persons. Penalties may include, but are not limited to, a letter of warning, a letter of reprimand, suspension without pay, dismissal, loss or denial of access to sensitive information (including National Security Information), or other penalties in accordance with applicable law and Agency rules and regulations, which can include criminal or civil penalties. Each case will be handled on an individual basis with a full review of all the pertinent facts. The severity of the security violation or the pattern of violation will determine the action taken.

b. Non-EPA personnel who knowingly, willfully or negligently disclose sensitive information to unauthorized persons will be subject to appropriate laws and sanctions.

APPENDIX B
APPLICATION RISK ANALYSIS AND APPLICATION CERTIFICATION

A. The Certification Process

Owners should review Section 2.4 before proceeding with this Appendix. That section contains information on combining applications for certification purposes. Owners should also note that in working through this Appendix a qualitative risk analysis is performed, that is, relative vulnerabilities and threats are assessed and safeguards are specified.

1. New Applications

Each new sensitive application must undergo initial certification and then re-certification every three years. This certification must take place prior to the application being put into use or production. The certification or recertification will begin with the application owner's completion of the Certification Worksheet, Exhibit B-1. The worksheet and specific instructions for completing it are described in Section B.

For PC applications, the Certifying Official, PC site coordinator, and PC custodian will be available to answer owner questions on an as needed basis. For minicomputer/mainframe applications, the Minicomputer/Mainframe Security Officer, the Systems Analyst, and the Applications Programmer must not only answer questions on an as needed basis, but they must also be an integral part of the process. The determination of security requirements and appropriate controls requires communication among all these parties. Safeguards to meet the owner's sensitivity requirements can be placed in the application itself and/or at the installation level. How the application is ultimately protected depends upon the safeguards already in place at the installation (and the results of the installation risk analysis) and the particular threats to the application.

After completing the worksheet, the owner will forward it to his/her immediate supervisor for review. The supervisor will review the worksheet for completeness and then forward it to the designated Certifying Official.

The Certifying Official will either certify that the application is adequately safe-

EXHIBIT B-1

CERTIFICATION WORKSHEET AND EXAMPLE

SENSITIVE APPLICATION CERTIFICATION WORKSHEET	
1. APPLICATION TITLE RCRA Settlement Offers	2. OWNER Ima Safe OSWER, OSW
3. TYPE(S) OF INFORMATION Enforcement confidential; high value	4. SENSITIVITY LEVEL & OBJECTIVE Confidential: Medium Level Availability: Medium Level
5. PROCESSING ENVIRONMENT Standalone; non-removable and removable media; shared user; Room 1123, West Tower, Washington, D.C.	6. DESCRIPTION Database application that tracks settlement offers by case. All users of PC may see confidential data.
7. SECURITY SPECIFICATIONS/REQUIREMENTS	
a. Controls to Maintain Availability - Back-up database to diskettes in accordance with the procedures manual. - Identify backup computing facility.	
b. Controls to Maintain Integrity (Minimal controls only)	
c. Controls to Maintain Confidentiality - Keep PC and removable media in a locked room. - Establish a formal list of authorized users.	
8. EVIDENCE OF ADEQUACY/DESIGN REVIEW - Check to make sure door lock installed. - Check to see that formal list of authorized users created. - Are backups created by user? - Memorandum outlining agreement for backup facility.	
9. TEST SCENARIO AND RESULT - Lock installed on 6-15-89. - List developed on 6-5-89. - Local backups kept in adjacent office; archival backup stored in Crystal City. - Memorandum with PC custodian in same branch executed 6-15-89.	
10. __X__ CERTIFIED	_____NOT CERTIFIED

guarded or deny certification by marking the appropriate box on the worksheet and returning it to the supervisor. A Certifying Official may conclude that safeguards are adequate if the application is protected in accordance with the procedures set forth in Sections 6-9 of this manual. When certifying the application, the Certifying Official must mark the appropriate box on the worksheet and sign the one-page certification statement shown as Exhibit B-2. These documents must be retained on file for inspection by OIRM, auditors, or the Office of the Inspector General.

Recertification of the operational application should be based on reviews or audits that test and evaluate the adequacy of implemented safeguards and that identify any new vulnerabilities. These reviews or audits should be considered part of vulnerability assessments and internal control reviews conducted in accordance with OMB Circular No. A-123.

2. Existing Applications

Each existing sensitive application must also undergo initial certification (and recertification every three years) in accordance with the instructions above. However, to avoid overwhelming organizations, initial certification may take place on a phased basis over the next two years. All initial certifications of existing systems should be complete by the end of 1991. More sensitive applications (as defined in Section 4) and those for which security plans were prepared (as described in Section 2.6) need to be certified first and as expeditiously as possible (by the end of 1990 at the latest). Because of their overall organizational knowledge, SIRMOs may be able to quickly prioritize applications for certification.

B. The Certification Worksheet

The certification worksheet should be completed by the application owner as follows. The numbers below correspond to the numbered blocks on the worksheet. The worksheet has been filled in with a PC application as an example of what is expected. In instances where major applications have many security requirements, owners may wish to reproduce the worksheet several times, using one copy for each individual requirement.

1. Application Title: Provide the name of the information system or application.

EXHIBIT B-2

CERTIFICATION STATEMENT

I have carefully examined the information presented on the Certification Worksheet for __(application name)__, dated _____. Based on my authority and judgement, and weighing any remaining risks against operational requirements, I authorize continued operation of ___(application name)___ under the restrictions/conditions listed below.

(List any Restrictions and Special Conditions or enter "None")

_____

_____

_____

_____

_____

_____

_____

_____

(Signature and Date)

2. Owner: List the application owner and organization.

3. Type of Information: Indicate the type of sensitive information (for example, CBI or high value) in terms of Section 4 of this manual.

4. Sensitivity Level and Objective: Provide the relevant security objective (for example, availability) and the associated sensitivity level (for example, high level).

5. Processing Environment: For PC applications, describe the processing environment in terms of shared versus single user PC, removable versus non-removable storage media, and standalone processing versus communicating with other equipment. Also indicate the physical and geographic location of the system. For other applications, describe the processing hardware, the communications configuration, the user community, and the physical and geographic location of the system.

6. Description: Provide a brief functional description of the application.

7. (a)–(c). Security Specifications/Requirements: For PC applications, express the needed availability, integrity and/or confidentiality security controls in terms of Section 7 of this manual. For other applications, describe the needed availability, integrity, and/or confidentiality controls in terms of Sections 6 and 9.

8. Evidence of Adequacy/Design Review: Indicate how the owner will ensure the security specs are being implemented.

9. Test Scenario and Results: Describe how the owner will satisfy himself/herself that the safeguards work or that the procedures are being followed.

10. Certifying blocks to be checked by the Certifying Officer as appropriate.

The application owner should note that the worksheet can also be used as a set of security procedures for the application's users. In other words, the worksheet can be used to communicate the sensitivity of the application and the security procedures to the user.

APPENDIX C
INSTALLATION RISK ANALYSIS

A. Background

A risk analysis is a means of measuring and assessing the relative vulnerabilities and threats to an installation. Its purpose is to determine how security safeguards can be effectively applied to minimize potential loss. In everyday terms, risk analysis is simply a procedure for identifying what could go wrong, how likely it is that things could go wrong, and what can be done to prevent them from going wrong.

Risk analyses may vary from an informal, qualitative review of a microcomputer or minicomputer installation to a formal, fully quantified review of a major computer center. For all Agency installations, including PCs and WP equipment, a qualitative approach may be used (see part C below).

B. Applicability and Required Schedule

All Agency installations, including PCs and word processors, are required to undergo a risk analysis. An installation risk analysis shall be performed:

- Prior to the approval of design specifications for a new installation. In the case of a PC or WP, the risk analysis shall be performed at the time the equipment is installed.
- Whenever a significant change occurs to the installation. For a PC or WP installation, significant changes include:
  - Physically moving the equipment to another location
  - Going from a single user to multiple users, or vice versa
  - Altering the communication configuration, for example, adding a dial-up capability or becoming part of a LAN.

  For a minicomputer/mainframe installation, significant changes include, but are not limited to:

  - Adding new equipment that is not the same as existing equipment
  - Adding new technology

– Adding dial-up capability

It is difficult to specify a precise set of criteria for identifying significant changes for mini/mainframe installations. At a large installation like NCC, adding hardware is commonplace and changing network definitions is also common; for the NCC, these do not constitute significant changes. If more guidance is needed to determine if a change warrants a new risk analysis, the Security Officer should consult his/her SIRMO.

- At least every five years, if no significant change to the installation necessitating an earlier analysis has occurred. Existing installations that have not undergone a risk analysis during the last five years must undergo one by the end of 1990.

C. Risk Analysis: Qualitative Approach

To perform the qualitative risk analysis required by this manual, the Security Officer or PC/WP custodian should complete the worksheet shown as Exhibit C-1 as follows. The numbers below correspond to the numbered blocks on the worksheet. The worksheet has been filled in for a hypothetical installation as a simple example of what is expected.

1. Location: Provide the physical and geographic location and the organization for the equipment.

2. Custodian and Equipment Type: List the person to whom the equipment is assigned and the type of equipment.

3. Type of Information: Indicate the type of sensitive information (for example, CBI or high value) in terms of Section 4 of this manual. If the installation does not process any sensitive information, the risk analysis is at an end and only the minimal controls set forth in Section 3 need to be implemented.

4. Number of Sensitive Applications: Indicate the number of sensitive applications processed at the installation.

5. Processing Environment: For a PC/WP, describe the processing environment in terms of shared versus single user, removable versus non-removable storage media, and standalone processing versus communicating with other equipment. For other installations, describe the communications environment, the users, the operating system, and installation hardware not described in 2 above.

6. Sensitivity Level and Objective: Provide the relevant security objective (for example, availability) and the associated sensitivity level (for example, high level).

EXHIBIT C-1

INSTALLATION QUALITATIVE RISK ANALYSIS WORKSHEET AND EXAMPLE

1. LOCATION Room 1123, West Tower OIRM	2. CUSTODIAN & EQUIPMENT TYPE R.U. Secure IBM 4381
3. TYPE(S) OF INFORMATION Enforcement confidential; high value	4. NUMBER OF SENSITIVE APPLICATIONS __2__
5. PROCESSING ENVIRONMENT Storage/communications capability located at OIRM; users limited to OIRM and other specifically authorized/trained personnel; OEM operating system.	6. SENSITIVITY LEVEL & OBJECTIVE Confidential: Medium Level Availability: Medium Level
7. CONTROLS TO MAINTAIN AVAILABILITY • Disaster recovery/continuity of operations plan developed. • Uninterruptible power supply installed. • List of personnel authorized to enter installation established. Visitor log developed; all visitors escorted during visit.	
8. CONTROLS TO PRESERVE INTEGRITY See items 7 and 9.	
9. CONTROLS TO PRESERVE CONFIDENTIALITY • Confidential hard-copy reports stored in a locked cabinet prior to distribution. Confidential reports are delivered by hand in sealed envelopes. • Unneeded confidential reports are shredded and outdated magnetic tapes with confidential data are degaussed. • Physical access control and visitor control are as described in 7 above.	
10. COMMENTS The procedures for all sensitive installations described in Section 6.4 have been implemented, including those related to password protection. RACF implemented for sensitive applications.	11. MINIMAL CONTROLS IN PLACE? _x_ YES ___ NO

7. Controls to Maintain Availability: Express the needed availability controls in terms of Section 6, 7, or 8 of this manual.

8. Controls to Preserve Integrity: Express the needed integrity controls in terms of Section 6, 7, or 8 of this manual.

9. Controls to Preserve Confidentiality: Express the needed confidentiality controls in terms of Section 6, 7,or 8 of this manual.

10. Comments: Self-explanatory.

11. Minimal Controls in Place: Indicate whether or not the minimal physical and environmental controls described in Section 3 are in place.

D. Risk Analysis: Quantitative Approach

In essence, a quantitative risk analysis is an exercise in cost/benefit analysis. Specifically, it involves the following steps:

- Identify the asset to be protected (equipment, application, data, etc.)
- Determine the threats to the asset
  - Natural, such as flood or earthquake
  - Man-made, such as fraud or accidental error
- Determine the probability the threat will be realized and the dollar loss (replacement cost, damages, etc.) if the threat is realized. Manipulate the two numbers to obtain the annual loss expectancy (ALE).
- Calculate the cost of security safeguards.
- Compare the cost of safeguards with the ALE and implement those controls that are cost-effective.

A simple example involving protecting a data base from fire follows:

- Asset is data base with a replacement cost of $20,000
- Threat is fire
- Rate of occurrence of fire is once every 50 years
- Annual probability of fire is 2%

- Annual Loss Expectancy is $400 (.02 x $20,000)
- Cost of safeguard (fire extinguisher) is $100 with a life of 5 years, or $20/year
- Obtain the fire extinguisher because it is cost-effective ($20 versus $400).

As the example shows, the concept of risk analysis is not difficult and is one the Agency already uses in formulating regulatory policy. What is challenging about risk analysis is identifying all the installation assets and threats and coming up with the needed dollar figures. Once these activities have been performed for the first analysis, however, subsequent risk analyses for the installation should be less time-consuming.

There are several different approaches for developing the numbers needed for a quantitative analysis. The procedures presented here are based in large part on Federal Information Processing Standard (FIPS) 65, entitled "Guideline for Automatic Data Processing Risk Analysis." Additional analytical concepts presented here are based on information in the HUD "ADP Security Procedures" handbook, the GSA "Automated Information Security" handbook, and the USDA "ADP Security Manual".

The approach outlined here should provide a reasonably accurate risk assessment, but other quantitative approaches may also provide accurate results. Security Officers may use alternative approaches if: (1) the approach includes the basic steps outlined at the beginning of this part, and (2) the approach yields all the information required for the risk analysis report (described in Step 5).

1. Step 1: Identify Assets and Determine Threats

Any risk analysis must begin with an inventory of installation assets. The essential first question is: "What potentially requires protection?" Basic categories of assets are as follows:

- Building (furnishings, detection systems, etc.)
- Supplies
- Hardware
- Communication Systems (equipment and service)

- Environmental "Systems" (power, air conditioning, etc.)
- Software (operating system and application)
- Data (source documents, output, files, data bases)
- Documentation and Procedures.

The threats to those assets must then be determined. To assist in this process, Exhibit C-2 has been developed. Exhibit C-2 is a simple matrix which presents assets by threats. To use the worksheet, put a check in each relevant square or matrix cell. For example, fire is a threat to hardware. Note that the threats have been tied to the three security objectives of availability, integrity, and confidentiality.

2. Step 2: Identify Existing Safeguards

The next step is to list all security safeguards that are currently in place. Each safeguard also needs to be tied to the asset it is protecting and to the threat it is counteracting. In other words, in terms of the Exhibit C-2 matrix, each safeguard should be tied to one or more squares or cells.

It is important to identify existing safeguards early, since additional controls can only be meaningfully selected in light of the existing security baseline. In addition, to the extent that threat/asset combinations are without corresponding safeguards, vulnerabilities are present. For example, if fire is a threat to hardware and there are no fire protection controls in place, the installation is vulnerable to fire.

3. Step 3: Calculate Annual Loss Expectancies

This step involves determining the annual loss expectancy (ALE) of each checked matrix cell. This calculation involves two components:

- Determining the probability the threat will be realized (or the frequency of occurrence)
- Determining the dollar loss if the threat is realized (the dollar impact of the occurrence)

Note that the frequency of occurrence implicitly incorporates how applicable the

EXHIBIT C-2

ASSET/THREAT WORKSHEET

Installation: Prepared by:

Date:

THREAT	Assets							
	Bldg.	Sup.	Hard-ware	Comm. Systems	Environ. Systems	Soft-ware	Data	Doc.
Availability:								
• Fire								
• Water								
• Storms								
• Earthquakes								
Environ. System Failures								
• Equip./System Failure								
• Theft								
• Accidental Data Destruction								
• Sabotage								
Confidentiality:								
• Unauthorized Disclosure								
Integrity:								
• Fraud								
• Sabotage								
Accidental Damage								

threat is. For example, if a threat is not relevant to an asset, the frequency of occurrence is zero.

To simplify the analysis without reducing its usefulness, the impact and frequency estimates should be rounded to the factors of 10 shown below. This is the approach recommended in FIPS 65.

- Impact:

$	10
$	100
$	1,000
$	10,000
$	100,000
$	1,000,000
$	10,000,000
$	100,000,000

- Frequency:

  100 times a day
  10 times a day
  1 time a day
  Once in 10 days
  Once in 100 days
  Once in 3 years (1000 days)
  Once in 30 years
  Once in 300 years

This kind of rounding is possible because it really makes little difference to the overall analysis if a threat is realized every 20 years or every 30 years. Similarly, the analysis is not significantly affected by an estimated dollar loss of $80,000 versus $125,000.

Impact and frequency estimates can be developed through interviews with Agency operational and technical experts. In many instances, common sense will be of great help. For example, in estimating the frequency of a wind storm, once in three years is probably too often and once in 300 years is probably too long. A more reasonable

estimate may be once in 30 years. Similarly, in assigning a dollar impact to fraud involving the payroll system, $1,000,000 is probably too much while $10,000 is too little. $100,000 is probably a reasonable estimate.

Oftentimes, impact and frequency estimates are more readily developed for physical or facility-related assets such as buildings or hardware. Estimates for assets such as data or documentation can involve more judgment, making the risk analysis conclusions for such assets less certain.

The ALE of a particular asset/threat combination is the product of the annualized frequency and impact estimates. To simplify the computation, Exhibit C-3 has been developed. Exhibit C-3 presents ALEs by impact/frequency combinations. For further convenience in performing the analysis, Exhibit C-4 has been developed. Like Exhibit C-2, Exhibit C-4 is a simple matrix which presents assets by threats. The cells in Exhibit C-4 should be filled not with checkmarks, however, but with ALEs. In other words for each checkmark in Exhibit C-2, there should be a corresponding ALE in Exhibit C-4.

In developing ALEs, two final items should be noted. First, in developing these estimates, do not factor in the effect of existing safeguards. For example, an existing fire detection system could reduce the dollar loss in the event of a fire, but to include that reduction here would muddy the analysis because it would assume the cost-effectiveness of the existing system. Instead, all ALEs should be developed as if there were <u>no existing</u> security controls. (The cost-effectiveness of existing safeguards is factored in later in the analysis.)

The second item to note is that in many instances it may be useful to make several copies of both Exhibits C-2 and C-4 and to create new asset headings on those copies. For example, Exhibit C-2 includes the assets "software" and "data." Within each of these categories, there may be several different data bases and applications, each with its own unique set of threats. In determining threats for applications and collections of information, always consult with the owner to find out the sensitivity designation and the relevant security objectives.

4. Step 4: Evaluate and Select Safeguards

To begin this final analytical step, identify the types of safeguards needed based on

EXHIBIT C-3

ALE by IMPACT/FREQUENCY COMBINATION

IMPACT	FREQUENCY							
	1 in 300 Years	1 in 30 Years	1 in 3 Years	1 in 100 Days	1 in 10 Days	1 in 1 Day	10 Per Day	100 Per Day
$ 10					$ 300	$ 3K	$ 30 K	$ 300K
$ 100			$ 300	3K	30K	300K	3M	30M
$ 1,000			$ 300	3K	30K	300K	3M	30M
$ 10,000		$ 300	3K	30K	300K	3M	30M	
$ 100,000	$ 300	3K	30K	300K	3M	30M	300M	
$ 1,000,000	3K	30K	300K	3M	30M	300M		
$10,000,000	30K	300K	3M	30M	300M			
$100,000,000	300K	3M	30M	300M				

Source: FIPS 65

EXHIBIT C-4

CALCULATING EXPECTED LOSS ALE WORKSHEET

Installation: Prepared by:

Date:

THREAT	Assets							
	Bldg.	Sup.	Hard-ware	Comm. Systems	Environ. Systems	Soft-ware	Data	Doc.
Availability:								
• Fire								
• Water								
• Storms								
• Earthquakes								
Environ. System Failures								
• Equip./System Failure								
• Theft								
• Accidental Data Destruction								
• Sabotage								
Confidentiality:								
• Unauthorized Disclosure								
Integrity:								
• Fraud								
• Sabotage								
• Accidental Damage								
Total								

the procedural guidance in Section 6. This is now the appropriate point to include existing safeguards, so make sure to factor those in to this process.

Once the safeguards have been identified, estimate their annual costs. Again, a high degree of precision is unnecessary. For example, if a physical access control system has a cost of $50,000 and a useful life of about 5 years, use $10,000 as the annual cost. Remember, however, that the cost of an existing control is only the annual maintenance cost and does not include the initial installation costs. Those initial costs have already been expended.

Construct alternative clusters of safeguards that address the threats to the installation's assets. Compute the costs, benefits, and overall cost-effectiveness of each set of safeguards as shown in Exhibit C-5.

Remember that most security measures are effective against more than one threat and will reduce the ALE of several different asset/threat combinations. Indeed, it is this characteristic that makes administrative and physical safeguards so cost-effective.

Experiment with various combinations of safeguards until a satisfactory aggregation is achieved. A satisfactory aggregation is one that: (1) addresses all important threats, (2) results in a significant reduction in the ALE, (3) creates overall benefits that are greater than costs, and (4) is affordable for the organization. A satisfactory aggregation need not drive the ALE to 0. Indeed, at an ALE of 0, it is possible that safeguard costs will exceed their benefits.

5. Step 5: Prepare A Report

Complete the risk assessment process by documenting the results. There is no standard length required. The report could be 10 pages long or 200 pages long, depending on the size and sensitivity of the installation. The report should include the following sections:

- Summary of Findings and Recommendations
- Introduction

EXHIBIT C-5

COSTS AND BENEFITS OF SAFEGUARDS

		Safeguard Set 1	Safeguard Set 2	Safeguard Set 3
(1)	ALE Now			
(2)	New ALE with Safeguards			
(3)	Benefits ((1) - (2))			
(4)	Safeguard Costs			
(5)	Cost-Effectiveness ((3) - (4))			

- Description of Existing Security Controls
- Discussion of Asset/Threat Combinations and the Overall Risk Profile of the Installation
- Findings and Recommendations
- Appendix Containing the Risk Analysis Worksheets.

APPENDIX D
DISASTER RECOVERY AND CONTINUITY OF OPERATIONS PLANNING

A. GENERAL

A disaster recovery and continuity of operations plan is required for each minicomputer/mainframe computer processing installation. Preparation of the plan is the responsibility of the installation's Security Officer. The Security Officer may delegate portions of this function to other knowledgeable individuals as long as the coordinating responsibility is retained.

These plans cover three distinct areas:

- Emergency Response Procedures: These are the actions taken during or immediately after an emergency to protect life and property and to minimize the impact of the emergency.
- Backup: This area involves two components: (1) establishing a routine schedule for backing up programs and data, and (2) determining where those programs and data would run in the event of an emergency. Taken together, the two backup components ensure the continuity of installation operations.
- Recovery: While the backup area focuses on establishing an alternative, temporary processing capability, the recovery area focuses on restoring a permanent, ongoing capability.

Clearly, disaster recovery plans are crucial for ensuring the continued availability of applications identified by owners as being critical or high value Agency applications. To the extent an installation does not process applications of this type, contingency planning is less important. Consequently, installations that only process applications involving confidentiality and integrity should focus primarily on emergency response and recovery; continuity of operations is relatively unimportant for these installations and may be omitted from their plans.

Each installation should prepare a plan in accordance with these procedures by the end of 1990. Plans should then by updated on an annual basis. Forward completed plans or updates to your organization's SIRMO.

B. STEPS TO DEVELOP THE PLAN

1. Step 1: Determine What Constitutes a Disaster

An emergency can vary from a temporary disruption of processing to the complete destruction of the installation. Determine what kinds of events will cause: (1) limited, temporary disruption, (2) major, serious disruption, and (3) catastrophic disruption. If the Asset Threat Worksheets were developed as part of the risk analysis, they can assist in this determination.

2. Step 2: Develop Emergency Procedures

Define and describe what needs to happen during and immediately after an emergency by developing procedures for:

- Notifying personnel of the emergency
- Responding to fire and other acts of nature
- Evacuating the installation
- Shutting the hardware down
- Protecting data and records.

These procedures must be written and must identify who will be responsible for what function during the emergency. All installation employees should have an assigned function during an emergency, which may be simply to evacuate the installation immediately and to remain home until called.

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

3. Step 3: Ensure Continuity of Operations

Based on owner sensitivity designations, develop a listing of critical and high-value applications. Establish a plan for data and software backup that includes frequency of backup, a retention schedule, and an off-site location for storage. The plan should recognize that transactions that have occurred since the last data backup may be lost and may need to be re-input. Make sure the plan is responsive to any special owner

requirements, such as more frequent backup than is typical.

Locate and execute an agreement for an alternative processing site to be used in the event of major or catastrophic damage. Because of cost and compatibility considerations, it is probably best to be backed-up by another installation at the EPA, for example, one Prime location backing-up another or WIC and NCC backing each other up. NCC can also back-up regional logical mainframe facilities and will consider backup arrangements for VAX and microVAX.

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

4. Step 4: Plan for Recovery

Develop a plan for re-establishing a permanent, on-going processing installation. Identify a new installation location in the event the old site cannot be rebuilt. Determine how hardware supplies and other needed items will be obtained. Determine how applications will be migrated back to the original processing installation or to the new installation.

5. Step 5: Testing and Training

Test the plan. For example, confirm compatibility with the backup processing installation by actually running a critical application there.

Train personnel in their emergency responsibilities.

6. Step 6: Prepare a Written Plan

Complete the process by documenting the plan. The report should include the following sections:

- Introduction
- Definition of Disaster for the Installation
- Description of Emergency Procedures
- Strategy for Ensuring Continuity of Operations (not required for installations with only confidentiality and/or integrity as objectives)

- Plan for Recovery
- Testing Procedures
- Training Plan
- Appendix Containing a Listing of Critical and High Value Applications at Installation.