EPA 2196 - INFORMATION SECURITY MANUAL FOR PERSONAL COMPUTERS

1993 Edition

. REFACE

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 EPA, the Agency information security policy is contained in a formal policy statement. (The policy statement, which was 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 exclusively with personal computer (PC) security. The second manual deals comprehensively with all types of information assets (paper records, mainframes and minicomputers, information systems, PCs, and word processors). 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.

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.

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 try to be as user friendly as possible in explaining to readers how to fulfill those responsibilities, the manuals are not painless. To ensure that information resources are adequately protected, the manuals 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

1. GENERAL INFORMATION

1.1 PURPOSE, SCOPE, AND APPLICABILITY

In accordance with the Agency's Information Security Policy, this manual establishes information security procedures for personal computers (PCs) 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 on PCs is adequately protected and that EPA organizations and employees are in compliance with all requirements of the policy.

This manual addresses PC security 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 stand-alone personal tool and/or it may function as a smart terminal in a communications configuration (such as PC to mainframe or in a local area network). This manual does not apply, however, to other types of microsystems such as word processors (for example, Lexitrons) or dumb terminals (those that are not programmable). Information security for these devices is dealt with in the Agency's comprehensive "Information Security Manual."

Consistent with the Information Security Policy, this manual applies to all EPA organizations and employees that use PCs. 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 systems on PCs.

The specific purposes of this manual are as follows:

- To save organizations money by making sure 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 crucial information were destroyed
- To help organizations meet internal control review requirements by providing them with a sound basis for assuring that automated PC information systems are adequately protected
- To assist staff in developing the system documentation required by the "EPA System Design and Development Guidance"

- To help organizations meet the security reporting requirements of the EPA PC planning process
- To enable organizations to undergo successfully 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 being 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 is an application that requires protection due to the loss or harm that could result from the improper operation or deliberate manipulation of the application itself.

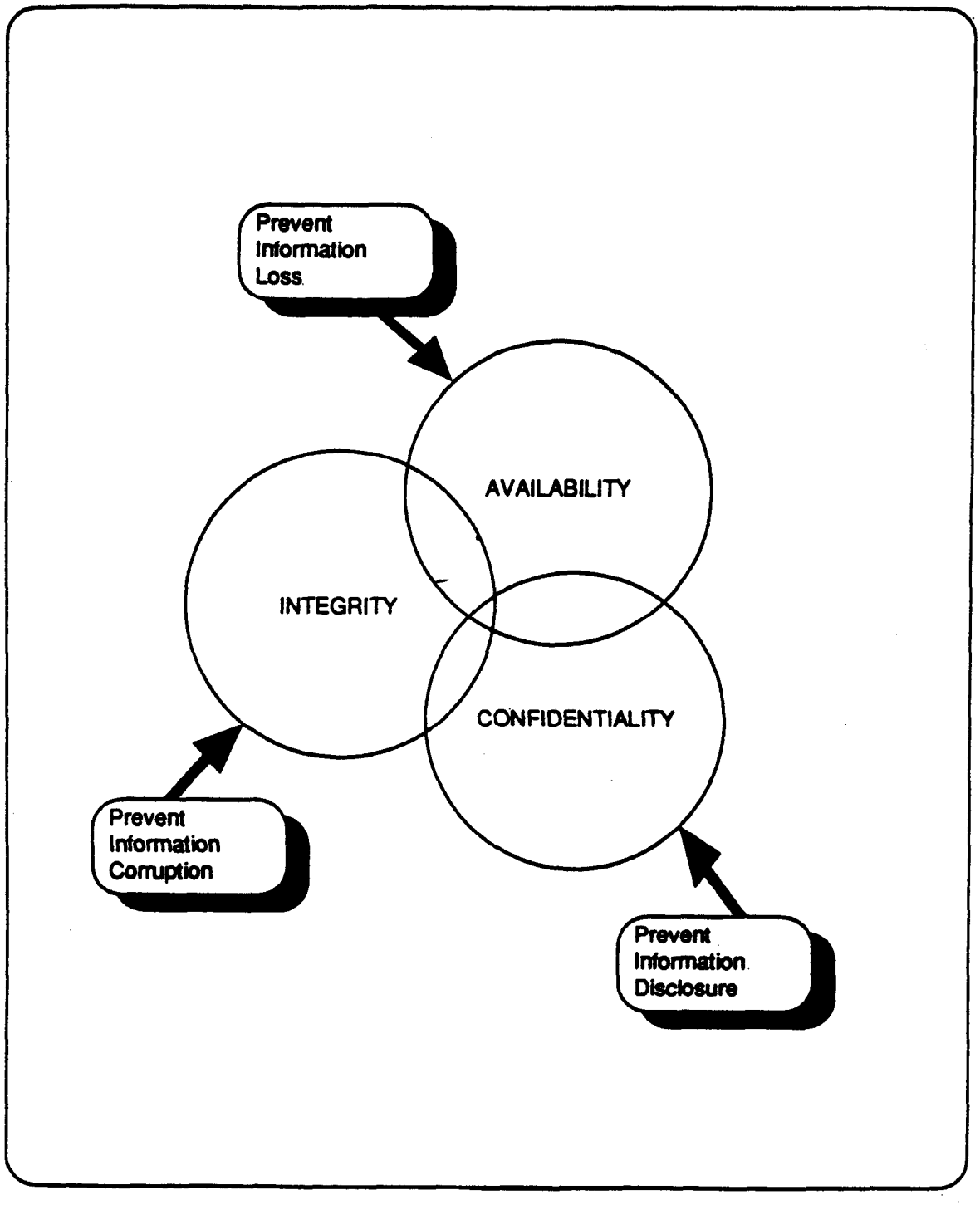
In short, information security involves the precautions taken to protect sensitive information resources from potential loss and misuse. The three major objectives of the EPA program, as illustrated in Exhibit 1-1, are to maintain:

- 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

EXHIBIT 1-1

INFORMATION SECURITY OBJECTIVES



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 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) Confidential Business Information (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 particular data base could contain information critical to a primary Agency mission and yet contain no confidential information. In other words, while availability is an objective, 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 PC SECURITY PROBLEM

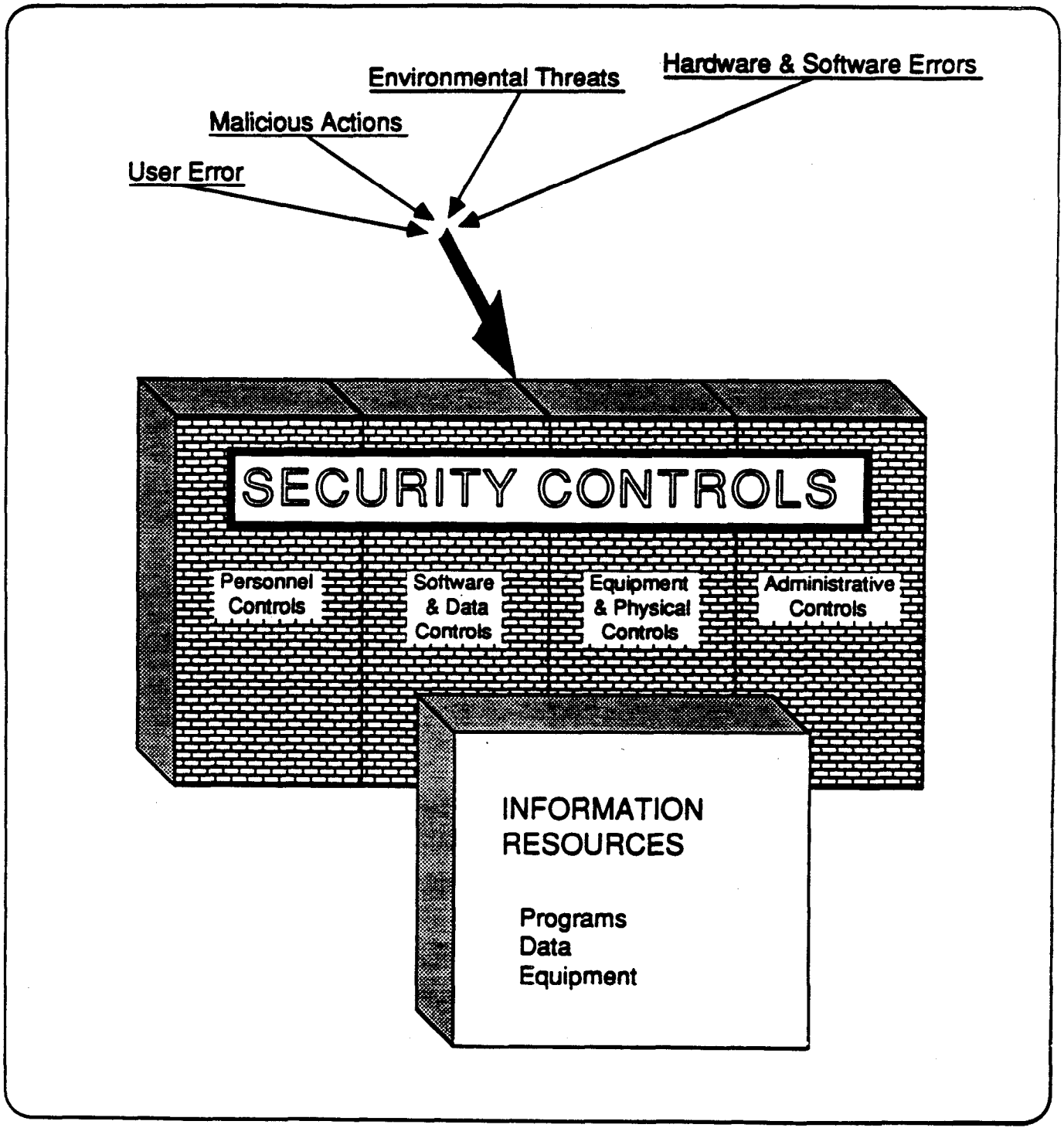
The expanding use of personal computers is creating major new opportunities for productivity improvement at the EPA. At the same time, however, this expanding use of personal computers is placing new information security responsibilities on office managers, research personnel, and others not previously recognized as 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.

The nature of the PC security problem is illustrated in Exhibit 1-2. A wide range of intentional or unintentional events can threaten information being stored and processed on a PC. These threats include:

External and environmental threats, such as fire, water damage, or power failure

EXHIBIT 1-2

THE SECURITY PROBLEM



- Hardware and software error, such as disk or operating system failure
- Operations error, such as accidental user modification or erasure of data
- Malicious actions, such as theft or data sabotage.

How vulnerable a particular PC is to these threats depends on two basic factors. The first is the type or nature of information being processed, that is, the relevance of each of the three security objectives. The second factor is the environment in which the PC is processing the information, for example, whether the PC is stand-alone or is 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.

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 or no 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.

1.4 STRUCTURE OF THIS MANUAL

PC security manuals are typically organized by type of security and include chapters on physical security, data security, communications security, and the like. While such manuals provide good technical discussions of security controls, they typically overwhelm the reader with a hodgepodge of safeguards that cause uncertainty about exactly which safeguards should be implemented. In addition, these manuals often provide little in the way of overall implementation guidance.

This manual is structured in a completely different manner. In essence, it is organized to allow each reader, whether a 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 concerns itself with individual and organizational information security responsibilities and should be read by all EPA managers and staff using PCs. 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 EPA organizational unit.

Section 3 describes minimal security controls to be used for all PCs, regardless of the processing environment or the type of information. Section 3 should also be read by all EPA managers and staff.

Section 4 is the last section that should be read by all EPA managers and staff. Section 4 analyzes the need for additional security controls by determining whether or not the reader has sensitive PC applications.

Based on the determination of sensitivity, the reader is referred to Sections 5-8, as appropriate. Section 5 highlights key personnel security considerations for those with sensitive PC applications. Section 6 addresses security procedures for those needing to maintain availability. Sections 7 and 8 present security procedures for those needing to preserve integrity and confidentiality, respectively.

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 PCs. 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, PC local area networks) 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 expand upon 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. PC 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 in a way that is not overly burdensome on programs and individuals. The remainder of this section describes a suggested overall framework for implementing the Information Security Policy as it relates to PCs.

The framework of security roles set forth in this section is <u>not</u> 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 PC 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, specific 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 System) Owner: The owner of the informati is the individual or organization who creates and sponsors it. Owne..ip 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 appro: ate, the owner specifies and approves security controls, and ensures tha application is protected on an ongoing basis. The owner also determines backup and availabi..y requirements and communicates them to the custodian.

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

- PC Custodian: The custodian is the individual to whom the PC is assigned. This is the person responsible for the PC in the property management sense.

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 so many different employees and supervisors, it is important to have one management official in each major organizational unit who can coordinate the security program for that organization. This individual will serve as a security focal point by identifying all PC 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 PC security function (for example, identifying PC owners, users, and todians) 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 five oversight roles. The first four of these roles exist at present while the remaining role is unique to the security program. The five roles are:

- Primary Organization Head
- First-line supervisors
- PC Site Coordinators
- Local Area Network (LAN) System Administrator
- Certifying Official: Management Official(s) appointed by the Primary Organization Head. This official certifies that the security safeguards that are in place for each sensitive application are adequate.

2.3 ASSIGNING RESPONSIBILITIES TO THE SECURITY ROLES: IMPLEMENTING PC SECURITY

Ensuring that PC information resources are adequately protected involves three different management control processes. First, basic, common-sense security measures need to be implemented for each PC, regardless of whether or not it processes sensitive information. Second, an application certification process needs to be established to determine the sensitivity of each PC application and to certify that the security safeguards for each sensitive application are adequate. Third, an installation risk analysis process needs to be established to make sure that the security measures in place for each PC adequately protect the sensitive applications stored and processed on the PC. 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 2-1 then lays out the security responsibilities associated with the processes on a role-by-role basis.

TABLE 2-1

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).
SIRMO	Coordinates the organization-wide security program. Identifies PC 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 Custodian	Responsible for the security of his/her equipment. Must implement minimal controls. Performs risk analysis.
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.

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 the PC and its magnetic media. Section 3 also sets forth administrative procedures governing the use of PCs and commercial software. Minimal controls are implemented by custodians or users as appropriate with oversight provided by the cognizant PC Site Coordinator.

2.3.2 Sensitivity Determination, Automated Application Risk Analysis, and 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 owner will determine the sensitivity of each of his/her applications. This determination will be made in accordance with the instructions set forth in Section 4 of this manual.
- Each sensitive application must undergo initial certification, and then review or audit leading to recertification 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 PCs 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, a 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 Agency PCs, a qualitative risk analysis approach will 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 the manual. If the PC does not process any sensitive information, the risk analysis is at an end and only minimal controls need to be implemented. If it does, 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 an installation risk analysis is the responsibility of the PC custodian. By working through this manual, an informal and qualitative risk analysis is performed. The custodian 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, custodians may feel that more rigorous, quantitative methods are warranted. OIRM does not wish to prohibit such thorough analyses. Interested custodians should review the last section of Appendix C for more information.

2.4 STREAMLINING THE IMPLEMENTATION OF PC SECURITY

In establishing these management control processes, OIRM wants to achieve adequate PC security throughout the Agency in a way that does not unduly burden 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 the organization's PCs and the information contained on them to function as a composite or aggregate owner, user, and custodian for the organization. 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 PC 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 or "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.

3. MINIMAL CONTROLS FOR ALL PCs AND PC LANS

3.1 INTRODUCTION

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 PCs and magnetic media, and 2) to set forth administrative procedures governing the use of PCs and commercial software. The dollar value of the typical PC configuration is usually several thousand dollars. All of the 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.

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 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 are required to prevent theft and physical damage. PC custodians are responsible for ensuring that these controls are in place.

- Locate PCs away from heavily travelled and easily accessible areas to the extent possible.
- When possible, install the PC in a locked room, making sure the lock is used whenever the room is unoccupied (and not just at night). If the PC 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 that 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 computers 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 measures already mentioned, store all portable PCs in locked cabinets when not in use. For further information or assistance, contact the Security Management Section of FMSD. Assign a person who tracks the location of the portable PCs on a regular basis, logs them out for use to authorized users, and ensures 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.

3.3 ENVIRONMENTAL CONTROLS

PC custodians are responsible for ensuring that the following controls are in place:

- PCs 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 PC 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.

- Computer equipment (and media) are sensitive to contamination from dirt, smoke, or magnetic fields. Do not eat or drink in the immediate vicinity of the PC. Per the Agency's smoking policy, do not smoke in the vicinity of the PC. (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 computer equipment with inexpensive plastic covers when not in use. Install the PC as far as practical from overhead water pipes or sprinkler heads.

- Control static electrical charges by placing antistatic mats under the computer 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.

3.4 MAGNETIC MEDIA CONTROLS

At present, virtually all information on microcomputers 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 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 the delicate surfaces and destroy data.
- Store diskettes in their jackets as soon as they are removed from the computer. 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 flexible 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.

3.5 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 a key file before realizing the importance of regular backups.

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 method 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), 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.

3.6 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. 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 PC only. With a site license, the software may be installed on more than one PC, typically for a higher fee. A copyright means that any unauthorized duplicating, selling, or other distribution of the software 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).

- Software purchased by the EPA must be used exclusively on PCs owned by the 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.

- Already established OIRM procedures concerning master copies of PC 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 WIC can be used for this purpose if an organization executes an Operational Service Agreement for Archiving of PC software.

3.7 UNAUTHORIZED USE OF PERSONAL COMPUTERS AND SOFTWARE

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

3.8 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 3.5) 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 PCs 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 the National Data Processing Division (NDPD) are also subject to the 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 the National Institute of Standards and Technology 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 personal computers and networks. A copy is available in the EPA Headquarters library or through the Government Printing Office.

4. DETERMINING THE NEED FOR ADDITIONAL CONTROLS

The minimal controls described in Section 3 are required for all Agency PCs. The purpose of this section is to determine whether or not additional controls are necessary.

Application owners use this section to evaluate the sensitivity of each of his/her applications. Determining sensitivity is an owner responsibility. If sensitive applications are owned, Section 6-8 need to be consulted, to develop the information required for the application certification process and the Application Certification Worksheet (see Appendix B).

Application users review this section to develop a working understanding of information sensitivity. Users can also use this section to determine the sensitivity of applications not yet evaluated by the owner (that is, existing applications that are undergoing certification). Section 6-8 should then be reviewed, as appropriate.

PC Custodians and LAN System Administrators review this section to develop a working understanding of information sensitivity. Custodians 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, and to identify the installation processing environment. Sections 6-8 then need to be used to determine what security controls must be in place and to develop the information needed for the Risk Analysis Worksheet (see Appendix C). This process constitutes a qualitative risk analysis and will ensure that adequate disaster recovery/continuity of operations plans are formulated.

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 for sensitivity determination purposes.

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

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.

If all questions can be answered "No" for all applications, the remainder of this manual does not apply. If any question can be answered "Yes" for any application, continueto determine how to protect the sensitive application(s) by completing the table. (After completing the table, make sure to have it reviewed as described in Section 4.4.)

The table has been designed as a worksheet for use in 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; use of these columns is explained below.)

4.2 DETERMINING RELEVANT SECURITY OBJECTIVES AND THE DEGREE OF SENSITIVITY

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

For each application, 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. Most high value PC applications will probably involve medium 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 turns out to be at both the 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 information (medium level confidentiality) would be of high level confidentiality.

TABLE 4-2

DETERMINING RELEVANT SECURITY OBJECTIVES AND DEGREE OF SENSITIVITY

Type of Information	Availability		Integrity		Confidentiality	
	High Level	Med. Level	High Level	Med. Level	High Level	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.*

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

4.3 DETERMINING THE PROCESSING ENVIRONMENT

Several of the procedural controls specified in Section 6-8 are described in terms of the environment in which the application or information is being processed. In using those sections, be alert to procedures that depend on three key environmental characteristics. As a result, answer the following questions for later use in implementing procedural controls.

- 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 diskette) 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 communications configurations applies:
  - Remotely Accessible by Modem (Dial-Up Capability)?
  - PC to Resource Server?
  - Local Area Network or LAN?

The security measures needed to maintain security in these different environments will be described in later sections. Regarding LANs, LAN System Administrators must note that the National Data Processing Division (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 procedures presented here. LAN System Administrators must make sure that they also comply with applicable NDPD policies.

4.4 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 and 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 applications as critical or high value. SIRMOs should be consulted when employees and supervisors need guidance in making a sensitivity determination.

4.5 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 6-8, is organized by information security objective:

- If availability is a security objective, review Section 6.
- If integrity is a security objective, review Section 7.
- If confidentiality is a security objective, review Section 8.

If more than one security objective is applicable (for example, an application where both availability and confidentiality are relevant), make sure to read the section pertaining to each applicable objective.

In discussing procedural controls, Sections 6-8 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.

5. PERSONNEL SECURITY AND TRAINING

5.1 INTRODUCTION

Given the large number of PC Custodians and users in the Agency, PC 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 offices. 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 potential 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 (OIG) and the Personnel Management Division, and 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.

Given the very definition of personal computing, it is often impractical to separate duties. The same individual often collects data, programs the application, tests the application, enters data and generates the reports. To minimize the potential for fraud, abuse, or sabotage, however, these duties should be performed by separate individuals to the maximum extent practicable. When it is not possible to have each duty performed by a different individual, try to separate the following: (1) data

collection/entry duties from application programming/maintenance duties, and (2) application programming duties from application testing duties.

In the case of PC-based financial applications (relating to check issuance, funds transfer, and the like) where misuse could cause loss, separation of duties is mandatory. 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 has to be removed or laid off, it is a good idea to rotate the employee to a non-sensitive position prior to giving the employee 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 are performed for personnel separating from sensitive positions:

- 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

OIRM is in the process of 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 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 the National Data Processing Division.

6. MAINTAINING INFORMATION AVAILABILITY

6.1 INTRODUCTION

This section 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 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 section describes threats, safeguards, and recovery procedures related to achieving the objective of maintaining availability. Subsection 6.2 catalogs and describes specific threats to information availability. Subsections 6.3 and 6.4 specify security measures for medium availability applications and high availability applications, respectively. The last subsection describes some steps that can be taken to recover from a processing disaster.

6.2 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.

6.2.1 Hardware Failure: Inability To Restart

Because of the generally high reliability of microcomputers, users tend to become overconfident and do 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 and it is necessary to repair or replace the drive, the data on the drive will probably be unavailable even after the system has been repaired.

6.2.2 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.

6.2.3 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 20 mb 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.

6.2.4 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.
- A dismissed employee may plant a "virus" in an organization's software prior to departure.
- An individual may feel that the automation of the individual's duties may make him or her more expendable.
- 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.

6.2.5 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 a key file before he/she realizes the importance of regular backups. Failure to perform regular backups is probably the most common and the most serious threat to availability.

6.3 PROCEDURES TO MAINTAIN MEDIUM-LEVEL AVAILABILITY

This subsection 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.

6.3.1 Lock-up Media

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

6.3.2 Write Protection

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

6.3.3 Isolated Storage

Isolate the critical/high value application on its own storage media to the extent possible. For an application residing on a floppy diskette, this means dedicating the diskette 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).

6.3.4 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 to Diskette 1.
  - On the second day, the data on the original diskette would be copied to Diskette 2.

- On the third day, the data would be copied to Diskette 1, writing 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 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, writing 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 should replace the one taken out of the backup loop. There may also be advantages in retaining several generations of the archival copies.

For Headquarters employees, the WIC is recommended as an off-site location. The WIC does charge a fee for storing backup copies, and 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.

6.3.5 Continuity of Operations

Backup computing facilities must be identified for critical applications and an agreement for 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).

6.4 PROCEDURES TO MAINTAIN HIGH-LEVEL AVAILABILITY

This subsection applies to applications that must be available continuously or within one day, and/or applications that are of very high value. All of the procedures set forth in Section 6.3 also apply here. The following additional procedures will be followed to maintain high-level availability.

6.4.1 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.

6.4.2 Manual Fallback

Identify and formalize manual data processing procedures to be followed in the event of a complete disaster in which the application is made unavailable.

6.4.3 More Frequent Backups

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

6.5 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 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. PRESERVING INFORMATION INTEGRITY

7.1 INTRODUCTION

This section 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 section discusses threats to integrity and procedures to safeguard and recover system integrity. The next subsection catalogs and describes specific threats to information integrity. Subsections 7.3 and 7.4 specify security measures for applications of medium-level integrity and high-level integrity, respectively. The last subsection describes some steps that can be taken to recover from data corruption.

7.2 THREATS TO INTEGRITY

7.2.1 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.

7.2.2 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 generally be considered to consist of a loss of data and would, therefore, represent an 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.

7.2.3 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 of the 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) PUB 73 and to the Agency's "Information Security Manual." FIPS PUB 73 is available in the Headquarters library or through the National Technical Information Service (NTIS).

This manual 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.

7.3 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.

7.3.1 Availability-Related Procedures

Adhere to all of the procedures described in Section 6.3, with the exception of those associated with continuity of operations. This will ensure that backups are created.

7.3.2 Confidentiality-Related Procedures

Adhere to the access control procedures described in Sections 8.3.2 and 8.3.3. Also, follow the password management practices outlined in Section 8.3.1. In addition, for PCs in a LAN, adhere to the procedures outlined in the following three 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 key 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.

7.3.3 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 mechanism from being bypassed.

7.4 PROCEDURES TO MAINTAIN HIGH-LEVEL INTEGRITY

All of the procedures set forth in Section 7.3 also apply here. In addition, the procedures listed below will be followed.

7.4.1 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.

7.4.2 Manual Fallback

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

7.4.3 More Frequent Backups

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

7.5 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.

8. PRESERVING INFORMATION CONFIDENTIALITY

8.1 INTRODUCTION

This section 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 8.3.3) 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 of OIRM.

The remainder of this section discusses threats to information confidentiality and procedures for safeguarding against disclosure. The next subsection catalogs and describes specific threats to confidentiality. Subsections 8.3 and 8.4 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 Sections 6 and 7, 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.

8.2 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 access 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 can 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 that have been used to print confidential reports.

- Unauthorized individuals can 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.

8.3 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 that follow are presented largely in terms of processing environment. Following a short subsection on controls that 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) 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 all pertinent organizational standards and procedures.

8.3.1 Procedures for all Environments

- Discourage traffic in the area where the computer is located when it is 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 the 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 logon 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 prevent 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.

8.3.2 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 USER 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.

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

Keep the computer under lock and key when it is not being used, that is, keep it in a locked cabinet and/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.

8.3.3 Procedures for Communicating PCs

This section applies to PCs that are connected to other equipment such as autoanswer modems, other PCs, or resource servers.

AUTOANSWER MODEM; SINGLE USER OR SHARED PC

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 it is 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 LAN or made available via a LAN unless specifically approved in writing by the Director of OIRM.

8.4 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.

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.

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

d. As a result, it is essential that an overall program be established to preserve and adequately protect the Agency's information resources. At the same time, it is equally essential that the program not unnecessarily restrict information sharing with other Federal agencies, universities, the public and State and local environmental authorities. Such information sharing has historically played a vital role in the overall fulfillment of the Agency 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.

Highly Sensitive: 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.

Other Sensitive: 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, which contains information on combining applications for certification purposes, before proceeding with this Appendix. 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. For sensitive PC applications, the certification or recertification will begin with the application owner's completion of the Certification Worksheet, Exhibit B-1. The form and specific instructions for completing it are described below. The Certifying Official, PC Site Coordinator, and PC custodian will be available to answer owner questions on an as needed basis.

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 safeguarded 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 6-8 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

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

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)

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 all of 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 FY 1991. More sensitive applications (as defined in Section 4) need to be certified first and as expeditiously as possible (by the end of 1990). 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 to provide an example of what is expected.

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

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: 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.

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

7(a) - (c). Security Specifications/Requirements: Express the needed availability, integrity, and/or confidentiality security controls in terms of Sections 6-8 of this manual.

8. Evidence of Adequacy/Design Review: Indicate how the owner will ensure that the security specifications 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 could 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, a qualitative approach may be used.

B. APPLICABILITY AND REQUIRED SCHEDULE

All Agency PCs are required to undergo a risk analysis. A risk analysis shall be performed:

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

EXHIBIT C-1

RISK ANALYSIS WORKSHEET AND EXAMPLE

1. PC LOCATION Room 1123, West Tower Washington, DC OSW	2. CUSTODIAN & EQUIPMENT TYPE R.U. Secure IBM PC/AT
3. TYPE(S) OF INFORMATION Enforcement confidential; high value	4. NUMBER OF SENSITIVE APPLICATIONS 1
5. PROCESSING ENVIRONMENT Standalone; non-removable and removable media; shared user	6. SENSITIVITY LEVEL & OBJECTIVE Confidential: Medium Level Availability: Medium Level
7. CONTROLS TO MAINTAIN AVAILABILITY • Remind users to backup data in accordance with the procedures manual. • Execute a memorandum with another PC custodian outlining agreement for backup computing.	
8. CONTROLS TO PRESERVE INTEGRITY (Minimal controls only.)	
9. CONTROLS TO PRESERVE CONFIDENTIALITY • Install a door lock. • Make sure application owner has established a list of authorized users.	
10. COMMENTS The procedures for all environments described in Section 8.3.1 have been implemented, except those related to passwords.	11. MINIMAL CONTROLS IN PLACE? x YES ___ NO

C. RISK ANALYSIS WORKSHEET

To perform the qualitative risk analysis required by this manual, the PC 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 PC to provide an example of what is expected. Note that the example involves the same application as that presented in Appendix B in order to highlight the differences in security perspective between owner and custodian.

1. Location and Equipment Type: Provide the physical and geographic location and the organization for the PC.

2. Custodian and Equipment Type: List the person to whom the PC 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 on the PC.

5. Processing Environment: Describe the processing environment in terms of shared versus single user PC, removable versus non-removable storage media, and stand-alone processing versus communicating with other equipment.

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

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

8. Controls to Preservee Integrity: Express the needed integrity controls in terms of Section 7 of this manual.

9. Controls to Preserve Confidentiality: Express the needed confidentiality controls in terms of Section 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. QUANTITATIVE RISK ANALYSIS

Detailed instructions for performing a quantitative risk analysis are contained in the Agency's "Information Security Manual."

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 database from fire follows:

- Asset is data base with a replacement cost $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).