NTAISS

NATIONAL
TELECOMMUNICATIONS
AND
AUTOMATED
INFORMATION
SYSTEMS
SECURITY

NATIONAL MANAGER

FOREWORD

This National Telecommunications and Information Systems Security Advisory Memorandum (NTISSAM) is intended to provide guidance to users, security officers, procurement officers, and others who are responsible for the security of office automation systems. This guidance is intended for use by all activities of the executive branch of the United States Government who process classified or sensitive, but unclassified, information in office automation systems. Other sources of guidance, including directives, manuals, and regulations issued by various departments and agencies of the United States Government are cited as references in the document.

Additional copies may be requested from:

Executive Secretary
National Telecommunications and Information
Systems Security Committee
National Security Agency
Fort George G. Meade, MD 20755–6000

This NTISSAM may be used or quoted without restriction.

Wm E Odom
WILLIAM E. ODOM
Lieutenant General, USA

EXECUTIVE SUMMARY

Office Automation Systems (OA systems) are small, microprocessor-based Automated Information Systems that are used for such functions as typing, filing, calculating, sending and receiving electronic mail, and other data processing tasks. They are becoming commonly used by managers, technical employees, and clerical employees to increase efficiency and productivity. Examples of OA systems include personal computers, word processors, and file servers.

This guideline provides security guidance to users of OA systems, to the ADP System Security Officers responsible for their operational security, and to others who are responsible for the security of an OA system or its magnetic storage media at some point during its life-cycle.

This guideline explains how OA system security issues differ from those associated with mainframe computers. It discusses some of the threats and vulnerabilities of OA systems, and some of the security controls that can be used. It also discusses some of the environmental considerations necessary for the safe, secure operation of an OA system.

This guideline suggests some security responsibilities of OA system users, and of ADP System Security Officers. Also described are some of the security responsibilities of the organization that owns or leases the OA system.

In addition, guidance is given to the procurement officer who must purchase OA systems or components, and guidance is also provided to the officer who is responsible for securely disposing of OA systems, components, or the associated magnetic media.

This document is issued as a National Telecommunications and Information Systems Security Advisory Memorandum, and is therefore intended as guidance only. Nothing in this guideline should be construed as encouraging or permitting the circumvention of existing Federal Government or organizational policies.

TABLE OF CONTENTS

PART I:

INTRODUCTION

1.0 INTRODUCTION

In recent years, there has been a tremendous increase in the number of Federal Government personnel using Automated Information Systems (AIS) to help with their jobs. In a large number of cases, the AIS involved are small, microprocessor-based systems referred to as “Office Automation Systems,” or “OA Systems,” for short. These OA Systems can increase efficiency and productivity of those whose jobs include such functions as typing, filing, calculating, and sending and receiving electronic mail. In addition, these systems can be used by technical and other personnel to performs functions such as computing and data processing.

When used wisely, OA Systems can be a boon to the office worker and the engineer alike, helping to get more work done in less time. Not using them in a secure manner, however, can result in the compromise, improper modification, or destruction of classified or sensitive, but unclassified, information (as defined in NTISSP No. 2 [18]). It is therefore necessary that OA System users be made aware of: (1) procedures and practices which will aid in the secure usage of these systems, and (2) the consequences of not employing security measures. The objective of this guideline is to address these two issues in the context of protecting classified or sensitive, but unclassified, information.

1.1 Purpose and scope

This document provides guidance to users, managers, security officers, and procurement officers of Office Automation Systems. Areas addressed include: physical security, personnel security, procedural security, hardware/software security, emanations security (TEMPEST), and communications security for stand-alone OA Systems, OA Systems used as terminals connected to mainframe computer systems, and OA Systems used as hosts in a Local Area Network (LAN). Differentiation is made between those Office Automation Systems equipped with removable storage media only (e.g., floppy disks, cassette tapes, removable hard disks) and those Office Automation Systems equipped with fixed media (e.g., Winchester disks).

1.2 Structure

This guideline is divided into four parts, which are further subdivided into a total of ten chapters. Part I is the introductory part of this guideline. Chapter 1 gives an introduction, while Chapter 2 discusses the Office Automation security problem and why it is different from security problems involving larger Automated Information Systems.

Part II provides guidance to the users of OA Systems. Chapter 3 details some security responsibilities of all OA System users. Chapter 4 provides guidance to users of stand-alone OA Systems, while Chapter 5 provides guidance to users of connected OA Systems.

Part III provides guidance to those ADP System Security Officers (ADPSSO) who are responsible for the security of OA systems. (Note: throughout this document, the term “security officer” will be used to mean ADPSSO.) Chapter 6 describes some of the responsibilities of security officers. Chapter 7 details some of the threats, vulnerabilities and security controls associated with Office Automation Systems.

Part IV provides guidance to others associated with OA Systems. Chapter 8 is a discussion of some of the security responsibilities incumbent upon the organization that owns an OA System. Chapter 9 provides guidance to procurement officers about addressing security during the procurement phase of the OA System life-cycle. Chapter 10 provides guidance concerning the disposal of Office Automation Systems and/or their components.

There is an Appendix that discusses security markings for the OA System and media used in it, a List of Acronyms that gives expansions for acronyms used in this guideline, and a Glossary that defines terms used in this document.

2.0 THE OFFICE AUTOMATION SECURITY PROBLEM

There are three major points to remember about Office Automation Systems when considering security of these systems throughout their life-cycle. These points are:

(1) Most current Office Automation Systems do not provide the hardware/software controls necessary to protect information from anyone who gains physical access to the system. Therefore, the most effective security measures to be used with these systems are appropriate physical, personnel, and procedural controls.

(2) All information stored on a volume of magnetic media (e.g., floppy disk, cassette tape, fixed disk) should be considered to have the same sensitivity level. This level should be at least as restrictive as the highest sensitivity level of any information contained on the volume of media.

(3) There are different security considerations for OA Systems with fixed media versus those with removable-media-only.

2.1 Protecting Information From Unauthorized Personnel

United States Government policy requires that classified information not be given to an individual unless he or she has the required clearance and needs the information for the performance of the job* [6, 20]. For sensitive, but unclassified, information, no clearance is required; therefore, all access is based solely on need-to-know [20]. These policies must be enforced for information contained within OA Systems as well as for all other information. Therefore, information contained in OA Systems must be protected from compromise, unauthorized modification, and destruction.

Most current Office Automation Systems processing classified or sensitive, but unclassified, information do not provide sufficient hardware/software security controls to prevent a user from accessing information stored anywhere in the system. Simply put, most current OA Systems are based on microprocessors that do not support multiple hardware states. In almost all cases, multiple hardware states are necessary to identify users, limit their actions, or keep them from accessing information for which they are not authorized. (See Section 7.5 of this document for a detailed discussion of this problem.)

In fact, at the time of this writing, no Office Automation Systems have been certified as meeting even the class C1 requirements listed in the Department of Defense Trusted Computer System Evaluation Criteria [2], (hereafter known as the TCSEC).

Because of the lack of adequate hardware/software security, proper physical, procedural, and personnel access controls must be used to prevent personnel from accessing the system while it contains any information (either in memory or on resident media) for which they are not authorized.

* Bracketed numbers correspond to References, p.57

2.2 Sensitivity Levels of Magnetic Media

All information contained on a volume of magnetic storage media should be considered to have the same sensitivity level. This sensitivity level should be at least as restrictive as the highest sensitivity level of any information contained on the media.

The reason for this requirement is simple: under ordinary circumstances, a user of an OA System has no way of knowing exactly what is written where on a volume of media. It is possible that there have been errors made in writing on the disk that result in parts of various files being combined without the user's knowledge.

> Example: On most magnetic disks, there is a file allocation table with entries pointing to where on the disk each file is stored. Compromise of data can occur if there is a cross-link; that is, if an entry in the file allocation table for one file actually points to part of another file. As files are accessed and modified, it is often not possible to write the entire file in a contiguous set of storage locations. Therefore, the file becomes fragmented. The more a disk is used, the more fragmented the files become, and the greater the probability of a cross-link. In order to guard against compromise of information due to a cross-link, all information on the disk is considered to have the same sensitivity.

It is also likely that classified or sensitive, but unclassified, information that has been “deleted” from the system is still resident on the media, unless it has been completely written over in an approved manner. (See Reference 4 for guidance on overwriting media.) Therefore, the media and all information on the media should be regarded as having a single sensitivity level.

It is certainly permissible to have some information on a volume of magnetic media that is actually less sensitive than the sensitivity level of the volume; however, due to the fact that it is impossible for the average user of an OA System to tell exactly what is written where, security dictates that this information be treated as having the higher sensitivity level.

> Example: Suppose that a floppy disk is marked “Personnel privileged information,” and there is a file on this disk that contains only unsensitive information, such as the General Schedule salary tables. While this unsensitive file is on the sensitive disk, it must be treated as sensitive, because bad pointers or other problems could cause the file to actually contain sensitive information. Further, this file CANNOT be copied to another floppy disk unless the second floppy disk is also considered to be sensitive, due to the possibility of “Personnel privileged information” unintentionally being copied.

If there is a file that is believed to be unsensitive that is stored on a sensitive disk, it is permissible to have a copy of that file printed, manually reviewed, and determined to be unsensitive. This paper copy can then be treated as unsensitive; however, the disk itself should still be considered to be sensitive. This applies to classified information as much as it does to sensitive, but unclassified, information.

2.3 OA Systems With Fixed Media vs. OA systems With Removable Media

“Removable media” are any magnetic storage media that are meant to be frequently and easily removed from the OA System by a user. Examples of removable media include floppy disks, cassette tapes, and removable hard disks.

“Fixed media” are any magnetic storage media that are not meant to be removed from the system by a user. Examples of fixed media include fixed disks and nonvolatile memory expansion boards.

An OA System with removable-media-only is one which meets both of the following criteria: (1) the system does not currently use fixed media (e.g., Winchester disks) to store or process information; and (2) other than removable media such as floppy disks or cassette tapes, the OA System must have only volatile memory. (In determining whether or not the OA System contains fixed media, any read-only memory (ROM) the system contains can be ignored.) If either condition is not met, the system should be regarded as containing fixed media.

The sensitivity level of an OA System with removable-media-only can be easily changed, because all classified and sensitive, but unclassified, information can be removed from the system after each use. This is not true of an OA System with fixed media--the sensitivity level of the system cannot be lowered without a great deal of effort, because it is virtually impossible to remove all classified and sensitive, but unclassified, information from the system. Therefore, if it is desired that the OA System be used to process information of several different sensitivity levels, or that it be used by personnel with different levels of clearances, an OA System with removable-media-only should be used. (See Sections 4.1.2.2 and 4.2.2.2 of this guideline for guidance on changing the sensitivity levels of OA Systems.)

PART II:

GUIDANCE FOR THE OFFICE AUTOMATION SYSTEM USER

3.0 RESPONSIBILITIES OF OA SYSTEM USERS

One of the most common problems in Information Security is determining exactly who is responsible for what. This is a particularly important issue when Office Automation Systems are involved, since there is much less opportunity for oversight of “average users” by “professional security people.” Therefore, it is incumbent upon each person to do his or her part to prevent the compromise of information.

The “average user” of an Office Automation System is the most important person in maintaining OA System security. If security is to be maintained, the user must develop a “security mindset” [16]. In view of this, the following general responsibilities of all OA System users are described. It should be remembered that responsibilities discussed in this section apply equally to each user of an OA System, regardless of whether or not that person has been formally designated as the security officer for that OA System.

(1) Each user of an OA System should know who the security officer for that system is, and how to contact that person.

(2) Each user of an OA System should have an awareness of the applicable security guidelines [5, 11,16, 23]. Users should follow the applicable guidelines. If it is necessary in an emergency to deviate from the security guidelines, the user should report this deviation to a security officer as soon as possible, so that the security officer can take appropriate action.

(3) In addition to violations of security procedures, each user should report suspected or known compromise of information and/or theft of property to a security officer [5, 23]. If a user believes that a part of the OA System (including software and magnetic media) is missing or damaged, or has been changed, and the user is unable to determine why and by whom the change was made, then the problem should be reported to the ADPSSO at once. Similarly, if a user has reason to believe that information may have been copied, modified, or destroyed improperly, the security officer should immediately be notified.

(4) It is the responsibility of each user not to use software provided by an unauthorized source. The user should not violate any copyrights or other license agreements, and is responsible for reporting any known violations to the security officer. Further, the user should not use any software which he has obtained without ensuring that it has first been thoroughly tested in an environment in which no operational information can be compromised or damaged.

4.0 OPERATIONAL SECURITY FOR STAND–ALONE OFFICE AUTOMATION SYSTEMS

4.1 OA Systems With Removable-Media-Only

4.1.1 Physical Access to Systems and Media

Physical access to the OA System at any given time should be limited to those with clearance and need-to-know for all information then contained in the system. It may be necessary to keep the OA System in a separate room or part of a room to keep unauthorized personnel from being able to read information displayed on the screen or on a printer. If the OA System is not in a protected area, special care should be taken to ensure that unauthorized personnel cannot gain access to sensitive, but unclassified, or classified information.

> Example: Kelly, who is in charge of office personnel affairs, must process the quarterly promotion list, which contains personnel information that must be protected under the Privacy Act of 1974 [20]. The OA System on which he must work, however, is located in the middle of the office, where several people who are not authorized to see the information can see what he is doing. Kelly should therefore take care to ensure that none of his co-workers can see the information he is processing. One way he might do this is to use partitions to surround the OA System and block the view of other employees. A second way is to position the CRT screen and printer in such a way that no one else in the office can see them, and then to ensure that no one is watching what he is doing. A third way is to make sure that the room is empty before doing his work.

It is important to emphasize that these rules also apply for personnel performing maintenance on the OA System. Maintenance, regardless of whether preventive or corrective, should only be done by authorized persons. Maintenance personnel should not be allowed physical access to the OA System until all classified and sensitive, but unclassified, information for which they do not have a clearance and need-to-know has been removed.

4.1.2 Using the Stand-Alone OA System With Removable Media Only

4.1.2.1 Normal Operation

The following procedures should be followed at all times during normal operation of the OA System:

(1) Monitor screens, printers, and other devices that produce human-readable output should be placed away from doors and windows. This helps ensure that casual passersby cannot read information from them [5, 8, 11, 19, 23].

(2) Never leave an OA System running unattended while it contains information that should not be seen by everyone with physical access to it. Especially, do not leave an OA System unattended while classified or sensitive, but unclassified, information is displayed on the screen. If a user must leave an OA System, he/she should follow the procedures outlined in Section 4.1.2.4 of this Guideline.

Example: Suppose that Tom edits a large data file containing personnel records on an OA System. When he is finished, he saves the edited file. Since writing the new file over the old one will take some time, Tom leaves the OA System to run an errand. Sue sees that the OA System is unattended, and accesses and modifies the personnel file, destroying its integrity.

(3) Electronic labels attached by the OA System to information on magnetic storage media should not be trusted to be accurate unless the OA System has been evaluated by the National Computer Security Center and has been found to be a B1 or higher trusted system. While it is a good practice to indicate the apparent sensitivity of information by an electronic label of some sort (e.g., by a character string in the file name or directory name, or by the value of the first byte in the file), these labels should not be trusted to be accurate. Therefore, all data on the media should be treated as being at a single sensitivity level--that which is indicated by the physical label attached to the media.

(4) It is not normally permissible to have a classified or sensitive, but unclassified, volume of magnetic storage media on line at the same time as a volume with a lower sensitivity level, unless the sensitivity level of the latter volume is immediately raised. (The exception to this is discussed Section 4.1.2.3.)

Example: Suppose that Terry has a file that she believes to contain only Unclassified information, but that is stored on a TOP SECRET floppy disk. Terry therefore copies the file to an Unclassified disk. The previously Unclassified disk should then become TOP SECRET. The reason for this is that there is no way for a user to determine exactly what has been written onto the disk; there is a chance that an error caused TOP SECRET information to be written onto the disk.

(5) Printers should not be left unattended while classified or sensitive, but unclassified, information is being printed unless the area in which it is located provides a level of physical security adequate to protect the printout from being read, copied, or stolen by an unauthorized individual.

(6) Any user who prints out classified or sensitive, but unclassified, information should remove that printout from the printer and/or printer area at the earliest possible time. If this is not done, classified or sensitive, but unclassified, information could be compromised by an unauthorized person reading, copying, or stealing a printout. (Note: this is particularly true if the printer is shared, and/or is not collocated with the rest of the OA System. Even if adequate physical security can be provided, it is good practice to remove the printout from the printer area at the earliest possible time.)

Example: Suppose that Pat is John's supervisor, and prints out John's personnel records on a printer. Pat then leaves the printout next to the printer, and leaves the room to attend a meeting. While Pat is gone, John's co-worker George walks into the room, notices the printout, and reads John's personnel records. This is a compromise of information, and is a violation of the Privacy Act of 1974 [20].

(7) The user should ensure that all printouts have appropriate sensitivity markings

(e.g., “Personnel Privileged Information,” “Proprietary,” “Confidential,” etc.) at the top and bottom.

(8) If the printer ribbon is used to print classified information, it should be marked at the highest classification level it was used for, removed from the printer when not in use and stored and otherwise protected and disposed of as any other classified item.

(9) Use only software that has been obtained from authorized sources. Do not pirate software yourself, and do not use any software which has been obtained by violation of a copyright or license agreement. Furthermore, software should not be used unless it has been thoroughly tested by someone trustworthy (such as the organizational software distribution office, or the ADPSSO) for errors and malicious logic before it is exposed to operational information. (This is especially true for software obtained from the public domain.)

(10) Do not eat, drink, or smoke while using the OA System. Any spillage could seriously damage the system and/or magnetic media.

(11) Protect magnetic media from exposure to smoke, dust, magnetic fields, and liquids. Diskettes that get wet will generally warp or become otherwise deformed. If a diskette or other volume of media does get wet, do not attempt to use it in an OA System, as doing so could result in damage to the system.

(12) If a manual audit log is kept for the system, record in it all necessary information.

(13) No information should be processed or stored on any OA System until a risk analysis has been completed and appropriate countermeasures have been determined.

(14) No classified information should be processed or stored on any OA System unless that system has been TEMPEST-approved for the zone in which it is operating [14, 15].

4.1.2.2 Changing the Sensitivity Level of Information the OA System is Processing

OA Systems using removable-media-only contain no fixed media, and therefore can be used to process information of different sensitivity levels. In some instances it may be more cost effective to simply process all information as being at the system high level, and then manually review all output for the proper sensitivity. However, if this is impractical, then the sensitivity level of the OA System may be changed. When a change in the sensitivity level is desired, the following steps should be taken:

(l) Remove all storage media from the system (this includes media containing both applications and systems programs).

(2) Power off the system, preferably for at least one minute. (This will allow any latent capacitance to bleed off, and ensure that memory is cleared. Again, the exact time required depends on the particular system used, and the system security officer should specify an

appropriate minimum time for systems under his/her control.)

(3) Power on and reboot the system with the copy of the operating system that is at the proper sensitivity level.

(4) Insert the applications media for the new sensitivity level into the system. There should be a different copy of the operating system, and of each applications package (e.g., a word processing package) for each classification of information the system processes (e.g., an Unclassified copy, a SECRET copy). It is recommended that there also be a different copy of the operating system for each sensitivity level of information the OA System processes (e.g., a "Personnel Privileged" copy, a "Company X Proprietary" copy). Each copy should be protected to a level appropriate for the sensitivity of information it is used to process.

There is one exception to this guidance. To use only one copy of an operating system or applications package for all sensitivity levels, the procedure is: first, boot the system or load the package with no classified or sensitive, but unclassified, information in the system. Then, remove the diskette or tape containing the software BEFORE any classified or sensitive, but unclassified, information is introduced into the system. DO NOT reinsert the software into the system until the sensitivity level of the system has been changed using the procedures described in Section 4.1.2.2

(5) The ribbon used to print classified or sensitive, but unclassified, information should be replaced by one used to print information of the new sensitivity level. The sensitive (or classified) ribbon should be either securely stored or disposed of, as appropriate.

4.1.2.3 Preparing Downgraded Extracts

In some instances, it may be necessary to copy some information from a volume of media at one sensitivity level to another volume that is at a lower sensitivity level (e.g., copy a file from a SECRET disk to an Unclassified disk). This is an extremely dangerous practice, and should only be done following the procedures that have been set by the security officer. Users should contact their system's security officer for specific guidance on preparing downgraded extracts of classified or sensitive, but unclassified, information.

4.1.2.4 When a User is Finished Using the OA System

When a user is through using the OA System, remove all removable media from the system and store it in a manner commensurate with information of that sensitivity. Record any audit trail information that may be required. If the system is used by more than one person at different times, it is advisable to power the system off at the conclusion of each person's use.

4.1.2.5 At the End of the Shift

At the end of the shift or workday, the following steps should be taken before leaving.

(1) Remove all removable media from the OA System.

(2) Overwrite each location in the system's memory with some pattern (e.g., all zeros, then all ones, then a random pattern) before the system is powered off.

(3) Power off the system. If there is a key, it should be stored in a secure place until the next shift or working day.

(4) Any printer ribbon that has been used to print classified or sensitive but unclassified, information should be removed, and either securely stored or properly disposed of.

The OA System should remain powered off during non-duty hours.

A checklist should be maintained that is signed or initialed at the end of each day to verify that the OA System has been properly shut down and removable media have been removed. This will assist in determining accountability for a discovered security problem.

4.2 OA systems With Fixed Media

4.2.1 Physical Access to Systems and Media

Physical access to the system should be restricted to those who are authorized access for all data currently being stored on the system. In addition, these users should be authorized access for all data that has been stored on the system since the system was last declassified. (See Reference 4 for declassification procedures.)

4.2.2 Using the Stand-Alone OA System with Fixed Media

4.2.2.1 Normal Operation

During normal operation of a stand-alone OA System with fixed media, all recommendations given in Section 4.1.2.1 which apply to the operation of an OA System with removable media are still applicable. However, additional vulnerabilities exist with OA Systems containing fixed media and therefore additional precautions must be taken.

Even though only one user can directly access the system at a time, it is likely that information originated by more than one user will be stored on the fixed media. Access to any classified information by a user not possessing a clearance or need-to-know for it is a violation of Executive Order 12356[6]. Access to certain other types of sensitive, but unclassified, information is contrary to the provisions of Section 3 of the Privacy Act of 1974 [20]. Systems which do not meet the requirements of at least class C2 cannot provide assurance of protection of information from anyone who gains physical access to the system. Therefore, if the OA System has been evaluated and found to be a class C2 or higher system, then the guidelines detailed in Reference 3 apply. Otherwise, all users should have proper clearance and need-to-know for all data that is stored or processed on the system.

Any removable media which is placed in the OA System automatically acquires the same sensitivity level as the system. However, if the original sensitivity level of the removable media is more restrictive than that of the OA System, the OA System and its fixed media acquire the more restrictive sensitivity level, and should be marked as such.

Example: Suppose that there is an OA System with one fixed disk and one floppy disk

> drive. The system and its fixed disk are classified SECRET. A previously Unclassified floppy disk placed in the system's floppy disk drive becomes classified SECRET. If a TOP SECRET floppy disk is placed in the floppy disk drive, however, the entire OA System and its fixed disk become classified TOP SECRET.

It should not normally be permissible to copy a file from a classified or sensitive, but unclassified, volume of removable storage media to a volume of fixed media with a lower sensitivity level, unless the sensitivity level of fixed media, and of the entire OA System, is immediately raised to the level of the removable media. (The exception to this is discussed in Section 4.2.2.3.)

> Example: Suppose that there is a file that is apparently Unclassified, yet it currently resides on a TOP SECRET diskette. If this file is copied to an Unclassified fixed disk, the sensitivity level of the previously Unclassified disk should now be TOP SECRET. The reason for this requirement is that we have no way of being sure exactly what is being copied; therefore, we must assume the worst case: that some TOP SECRET information may be inadvertently copied onto the Winchester disk. Therefore, the sensitivity level of this previously Unclassified disk should be raised.

Furthermore, it should not be permissible to copy a file from a classified or sensitive, but unclassified, volume of fixed media to a volume of removable media with a lower sensitivity. If this does occur, the sensitivity of the removable media should be immediately raised.

Information that individual users wish to protect from other users of the OA System should be stored on removable media. This removable media can then be appropriately protected when it is not in use. This recommendation stems from the fact that OA Systems that do not meet the TCSEC requirements for at least class C1 cannot prevent any system user from gaining access to any location in the system's memory, to include the locations where the hardware/software controls themselves are stored. If the information is removed from the system along with the media it resides on, however, it cannot be accessed by others. (However, users should be very careful, as quite often information is left on the fixed media in the form of scratch files or backup files.) Users should make sure that media they remove from the OA System are properly secured. For example, if a floppy disk is removed, it should be locked away, not left lying on top of a desk or put in an unlocked container. One of the conditions for security is that adequate physical protection must be provided; if it is not, then all information is vulnerable.

4.2.2.2 Changing the Sensitivity Level of Information the OA System Is Processing

It is not permissible to lower the sensitivity level of the OA System unless it has been declassified using the procedures described in Reference 4.

Unless the OA System meets the requirements of at least class B1 when evaluated against the TCSEC, it should not be used to process multiple sensitivity levels of information simultaneously. In this case, it is not permissible to change the sensitivity level of the information the OA System is processing. Any information which is being processed by the OA System must be regarded as having the same sensitivity level as the system itself, regardless of its apparent sensitivity.

4.2.2.3 Preparing Downgraded Extracts

In some instances, it may be necessary to copy some information from a volume of media at one sensitivity level to another volume that is at a lower sensitivity level (e.g., copy a file from a SECRET disk to an Unclassified disk). This should only be done following the procedures that have been set by the security officer. Users should contact their ADPSSO for specific guidance on preparing downgraded extracts of classified or sensitive, but unclassified, information.

4.2.2.4 When a User is Finished Using the OA System

If there are any classified or sensitive, but unclassified, files stored on the fixed media that other users of the system should not be able to access, they should be removed from the system[8,9]. First, copy the files to a volume of removable media. Then, remove the information contained in these files from the fixed media by overwriting each location that contained these files with some pattern (e.g., all zeros, then all ones, then a random pattern) [8, 9]. The software that is used to do the overwrite should be trusted to a level commensurate with the OA system level of sensitivity.

4.2.2.5 At the End of the Shift

See Section 4.1.2.4. All safeguards described there are equally applicable to OA Systems with fixed media.

In addition, the OA system itself should be physically secured in some way. If the room containing the OA system is approved for open storage of classified information at the highest level of information contained on the OA System, it may be sufficient to secure the room in the appropriate manner. If the room is not approved for open storage of classified information, then the OA System itself should be secured by locking it in an approved cabinet.

5.0 OPERATIONAL SECURITY FOR CONNECTED OFFICE AUTOMATION SYSTEMS

(Note: In addition to the guidance given in this section, all guidance given in Chapter 4 of this guideline is also applicable, and should be followed whenever the OA system is used.)

5.1 Using an OA system as a Terminal connected to Another Automated Information system

When an OA System is used as a terminal, all of the normal rules for connecting terminals to AIS should apply[10]. For example, these rules should include never leaving the OA System unattended while it is connected to another AIS, unless a software locking mechanism is used which prevents anyone, not passing an authentication check, from interacting with the remote AIS.

5.1.1 Office Automation Systems Versus "Dumb Terminals"

Office Automation Systems used as terminals can cause security problems that do not occur when "dumb terminals" (i.e., those that are not programmable) are used. Among these are the possibility of malicious communications software in the OA System, and the ability of the OA System to store such things as passwords.

Users of OA Systems should be wary of untested communications software. The organization owning the OA System should take any steps practicable to ensure that communications software used with their systems does exactly what its documentation claims, and nothing else. In general, at least one copy of the software should be tested, either by someone within the organization or by someone outside of the organization who can adequately test software.

If communications software is used that contains malicious code, the communications software can cause information (including the user's password) to be compromised, can corrupt information flowing between the OA System and other AIS, or can cause service to be denied completely. Worse still, it can do much of this without the knowledge of the person using the software. Therefore, it is very important not to use communications software packages that have not been approved for use by a responsible security officer.

Under no circumstances should a user's password for any remote AIS ever be stored in an OA System [11]. While it may seem convenient to program the OA System to execute the login routine on a mainframe computer system for you, it is important to remember that the OA System can also execute the same routine for someone else. This can result in another user of the OA System being logged into a remote AIS as you!

> Example: Suppose that Janet programs her personal computer so that when she is communicating with the AIS called MAINFRAME and presses the CONTROL and BREAK keys at the same time, her PC sends out her user-identifier and password to MAINFRAME. In other words, the PC executes Janet's login routine on MAINFRAME for her. She thus saves the keystrokes involved in typing the information each time she logs in, and doesn't even have to remember her password!

The problem occurs when Pat sees what Janet does, and decides to take advantage of this "user-friendliness." When Joe is not around, Pat simply connects Janet's PC to MAINFRAME, presses the CONTROL and BREAK keys simultaneously, and is now logged onto MAINFRAME as Janet. Once this happens, there is no way to prevent the compromise of information, since MAINFRAME has no way of knowing that it is not really Janet at the other end of the terminal!

In summary, storing a password in an OA System is the same as writing it down on a piece of paper--if anyone ever finds it, the security that was to be provided by that password has been defeated.

5.1.2 Consequences of Removable Media vs. Fixed Media

Because the sensitivity level of an OA System with fixed media cannot be easily changed, it is difficult to use one of these systems as a terminal to a wide variety of other AIS, particularly if each of these remote AIS is processing information of different sensitivity levels. Therefore, once an OA System with fixed media is connected to an AIS processing classified information, that OA System should be considered to be classified. It should NOT be connected at a later time as a terminal to an AIS that is not approved to process information classified at the same or a higher level.

An AIS with removable-media-only, however, can more easily be used as a terminal to, for example, a SECRET host at 2:00 pm and an Unclassified host at 4:30 pm, because its sensitivity level can be changed. If you are using an OA System with removable-media-only, and it is necessary to connect to an AIS that is processing a different sensitivity level of information than the last AIS that the OA System was connected to, the sensitivity level of your OA System should be changed in accordance with Section 4.1.2.2 of this guideline.

5.2 OA systems Used as Hosts on Local Area Networks

Suppose that there is an OA System attached to a Local Area Network (LAN). It is important for both the user and the security officer to understand that, as a general rule, any person who can access any other component of that LAN can access any information contained in that OA System. This includes any information that is stored on both fixed and removable media that are currently contained in the system, and applies regardless of whether the person is accessing the OA System from its keyboard or over a network. Therefore, the problem of compromise of information to an unauthorized individual is greatly increased any time an OA System is connected to a network. For this reason, the user should NEVER leave the OA System while it is logged in to the LAN.

5.2.1 Consequences of Removable Media vs. Fixed Media

If some information in the OA System is stored on removable media, those media can be removed from the system so that the information cannot be accessed by a remote user. If the information is stored on fixed media, it cannot be easily removed from the system, and the owner of the information should be aware of its vulnerability to compromise.

Suppose that there is an OA System that does not meet the class B1 requirements and that is used as a LAN host. Any information that should not be shared with every user of the LAN should be stored on removable media, and these media kept out of the OA System when this information is not needed.

If the OA System meets the requirements of class B1 or higher, then these media may be left in the system.

5.2.2 Controlling Access to System Resources

In order to prevent the compromise of information, access to the resources of the LAN and of each OA System connected to it should be controlled. These controls may include physical, procedural, and hardware/software features, or some combination thereof.

One way to ensure that information is not compromised is to provide such hardware/software features as access control, identification and authentication, and audit. If these features are provided, and the network as a whole can be trusted to prevent users from gaining access to information for which they are not authorized, then the other controls needed for security (e.g., procedural controls, physical access controls) are similar to those required for stand-alone OA Systems.

However, since the hardware/software controls necessary to provide security in a LAN are often unavailable, procedural controls should be implemented. These include:

(1) Have all OA Systems connected to the LAN operate at the same sensitivity level. That is, there should be no information processed anywhere on the LAN that some user of the LAN does not have a clearance, formal access approval, and need-to-know. Users should make certain that they remove from their OA Systems any media containing information that they do not want to share with each other user in the LAN.

(2) Provide specific LAN-oriented physical access controls. Instead of keeping unauthorized personnel away from a single OA System, it is now necessary to keep them away from all OA Systems that are connected to the LAN. Some of these OA systems may be located or may have peripheral devices (e.g., shared laser printers) that are located in public areas. Therefore, each user must help to ensure that no one is using any part of the LAN without authorization. Further, each user should pick up any human-readable output from any shared devices as soon as possible. For example, printouts should not be left in the printer room for six or eight hours if the room is not sufficiently protected to keep unauthorized personnel from gaining access to classified or sensitive, but unclassified, information. A good rule of thumb is, if you don't want others to read a sensitive file, do not leave it where it can be seen.

PART III:

GUIDANCE FOR ADP SYSTEM SECURITY OFFICERS

6.0 RESPONSIBILITIES OF THE ADPSSO

There should be one individual who is responsible for the security of each Office Automation System [5,11]. This individual may be one of the users of the system itself, or he/she may be a person who has responsibility for the security of all OA Systems within the organization. (It should not be the OA System manager, due to the potential lack of accountability.) Regardless of who the individual is, the ADPSSO has certain responsibilities which must be carried out in order to ensure that the OA security policy is enforced. These include:

(1) Ensuring that each OA System is certified and accredited, if required by organization policy.

(2) Ensuring that all users of the system are aware of the security requirements, and assuring that all procedures are being followed.

(3) Investigating all reported or suspected security violations, and determining (to the best of his/her ability) what has happened.

(4) Reporting violations to appropriate authorities (e.g., top management, agency security officers, etc.).

(5) Ensuring that the configuration management program is followed. He/she should approve maintenance before it is done, and ensure that no changes are made to either the hardware or software of the system without approval.

(6) Reviewing the audit logs for anomalies (if audit logs are used).

(7) Enforcing (and possibly also developing) procedures by which downgrading of information contained on magnetic media can be done, if the organization permits such downgrading.

7.0 THREATS, VULNERABILITIES AND CONTROLS

7.1 Threats, Vulnerabilities, and Controls: an Overview

The security officer of any OA System should have a familiarity with some of the security issues involved with that system. This chapter will give the security officer that familiarity.

In computer security terminology, a threat is a person, thing, or event that can exploit a vulnerability of the system. Examples of threats include a maintenance man who wants information to sell, a wiretapper, or a business competitor.

A vulnerability is an area in which an attack, if made, is likely to be successful. Examples of vulnerabilities include lack of identification and authentication schemes, lack of physical access controls, and lack of communications security controls.

If a threat and a vulnerability coincide, then a penetrator can cause a violation of the system's security policy. For example, suppose that there is a maintenance person (the threat) who is secretly working for an unscrupulous contractor. In addition, there is a vulnerability in that lack of physical access controls allows maintenance personnel to work on the OA System without supervision. In this case, information may be corrupted, causing a disruption in the normal work routine.

A security control is a step that is taken in an attempt to reduce the probability of exploitation of a vulnerability. This control may take one of many forms: an operational procedure, a hardware/ software security feature, the use of encryption, or several others.

There are many possible threats to the information being stored by an Office Automation System, as well as to the system itself. The system may be stolen or destroyed. Information stored on the system may be compromised; that is, it may be exposed to a user or process that does not have proper authorization to see it. Information may also be corrupted or destroyed altogether by a malicious user. Another threat might be the interference with the system’s ability to process information correctly. It is the purpose of this document to educate the security officer and the user as to the proper defenses against each of these threats. The following is a breakdown of some of the security issues involved in combating each of several types of threats.

7.2 Physical and Personnel Security

7.2.1 Physical and Personnel Security Threats and Vulnerabilities

In many instances, there is a danger that classified or other sensitive, but unclassified, data being processed in an OA System will be exposed to someone without a proper clearance or authorization for it. This is particularly true if the OA System is not physically located in an appropriate area, or if an OA System is directly accessible to external users by a communications line.

(An “appropriate area” is one that is approved for the highest level of information that has ever been processed or stored on the OA System.)

For the purposes of determining the level of security needed for an OA System, the following rule should be used:

> Any information that can be accessed using the communications capability of an OA System should be regarded as being processed by that OA System.

This may mean that a more stringently controlled area is needed for a particular OA System, or that certain communications should not be allowed.

> Example: Suppose that there is an OA System physically located in an area that is approved for no higher than SECRET information. If the OA System is connected to another AIS that contains TOP SECRET information, and the remote AIS is not trusted to separate TOP SECRET and SECRET information, then the OA System should be regarded as processing TOP SECRET information. In this case, there are two things that can be done: not allow the connection of the OA System to the remote AIS, or upgrade the physical surroundings of the OA System so that TOP SECRET information may be stored there, and institute physical and procedural controls to ensure that only personnel with TOP SECRET clearances can gain physical access to the OA System.

Regardless of the physical area in which the OA System is located, it is possible that all or part of the machine can be stolen or modified. The theft of a hardware part of the system may result in damage being done to the owning organization, since many times it is possible to recover residual information directly from the hardware

7.2.2 Physical Access Controls

The OA System should be located in an area that is approved for data as sensitive as the highest level of information it has stored or processed since all of its fixed media and semiconductor media were last declassified. Further, any other AIS or AIS component that can access the OA System should also be located in an area that is approved for this highest sensitivity of information.

> Example: Suppose that an OA System is used to process TOP SECRET data. This system should be stored in an area that is approved to store at least TOP SECRET material. (This requirement holds even if some or most of the information processed on the system is classified at a lower level than TOP SECRET.) Any other AIS or AIS component that is logically connected to this OA System must also be kept in an area that is approved for TOP SECRET data.

Regardless of the physical area in which it is located, the OA System should be marked with the most restrictive sensitivity of information that may be processed on it. (See the Appendix of this Guideline for detailed guidance on the marking of OA Systems.)

The OA System itself should be protected in such a way that sufficient protection is provided against theft or destruction of the system or its components. Possible precautions that can be taken include locking the OA System and its peripheral devices to a table, locking it in a cabinet, or keeping it in a locked room or vault. Any apparent theft or destruction of the OA System or any of its components (to include software) should be reported immediately to the security officer.

7.2.3 Personnel Security Controls

Executive Order 12356 states that "A person is eligible for access to classified information provided that a determination of trustworthiness has been made by agency heads or designated officials and provided that such access is essential to the accomplishment of lawful and authorized Government purposes" [6]. The Privacy Act of 1974 states that no agency may disclose privacy information to any person without the prior written consent of the person to whom the information pertains, except for a limited set of purposes[20]. In order to meet these and other policy-based requirements, only personnel who possess the proper clearances, formal access approvals, and need-to-know for all information then contained in the OA system should be allowed physical access to the system. Under ideal circumstances, maintenance or configuration changes that must be done by vendor or support personnel should only be done by personnel who are cleared for and have a need-to-know for all information then contained in the system. If this is not possible, then vendor or support personnel should be escorted by someone who is cleared and has a need-to-know for all information on the system. If the OA system or parts of it must be sent to another location for repair, care should be taken to ensure that no one without the proper clearances and need-to-know for information previously contained (or possibly contained) in the system at any given time has access to the OA System at that time.

7.3 Communications Security

7.3.1 Communications Security Threats and Vulnerabilities

Communications Security vulnerabilities are those that can be exploited whenever an Office Automation system has the capability to electronically send information to or receive information from another AIS. These vulnerabilities exist primarily in two areas: (a) interception of information during transmission, and (b) non-detection of improper messages and message headers received by the OA System.

Whenever an OA System is used to electronically send information to or receive information from another computer system, there is a chance that the information will be compromised by being intercepted while en route. Therefore, steps should be taken to ensure that no information is compromised during transmittal.

In addition to the problem of compromise, an OA System receiving information from another system should have some amount of assurance that the message and its header are authentic--that is, the receiving OA System is not being tricked into believing a false header. The integrity of messages and control information is crucial to the secure operation of a network. If a message were to be received with a phony header that was not detected, it could cause the system or a human using that system to take some action that would violate the security policy. Therefore, any forged messages or message playback should be detected by the OA System or by the network it is connected to.

For additional information, please contact your organization's Computer Security Office. Additional information is available from NSA, 9800 Savage Road, Ft. George G. Meade, MD 20755–6000, Attention: DDI.

7.3.2 Communications Security Controls

Regardless of whether the system is being used as a terminal attached to a mainframe or as a host attached to a local area network, either encryption or physically protected communications media should be used whenever the OA System is used for the communication of classified information. This protection must be sufficient for the highest classification of data that will be transmitted over the communications media.

Encryption should be used to protect information from being compromised any time it is not possible to physically protect the communications media. In addition, cryptographic techniques may be considered even when communications media can be physically protected only help prevent compromise of information by interception, it will also help prevent spoofing. Cryptographic checksums can be used to verify the integrity of the message and its sender.

The term “physically protected communications media” means that the media (e.g., the communications lines) cannot be accessed by a system penetrator (that is, they are immune to a hostile wiretap, either active or passive), and that TEMPEST considerations do not raise a significant problem in the specific environment. An example of physically protected communications lines is communication cables that are physically located within a secure area and are used to connect OA Systems in a LAN.

7.4 Emanations Security

Under certain circumstances, it is possible to detect what information is being processed by a computer system by analyzing the electromagnetic emanations coming from the system. This could result in the compromise of classified or sensitive, but unclassified information. To prevent this OA Systems that process classified information must be protected in accordance with the National Policy on the Control of Compromising Emanations. For specific applications see NACSI 5004, “TEMPEST Countermeasures for Facilities Within the United States (U)” [14], and NASCI 5005, “TEMPEST Countermeasures for Facilities Outside the United States (U)” [15]. (Note: The **entire** OA System must be protected. Connecting a TEMPEST approved CPU, monitor, printer, and keyboard together with an unapproved cable or without due regard for proper RED/BLACK separation and installation criteria can result in the failure of the entire system to meet the TEMPEST requirements.)

7.5 Hardware/Software Security

7.5.1 Hardware/Software Threats and Vulnerabilities

Hardware/Software vulnerabilities are those that can be exploited because of the inability of the OA System’s hardware, software, and firmware to prevent users from accessing data in or controlled by the system.

The threats to exploit these vulnerabilities generally fall into one of three general categories: compromise of classified or sensitive, but unclassified, data; unauthorized modification or destruction of data; and denial of services to authorized users. More specifically, an unauthorized user can access data, can modify data, or can deny use of the data or even the OA System itself to authorized users.

If an OA System is networked, the vulnerability of data is greatly increased. First, a user of one OA System may be able to access another AIS, and data that was previously inaccessible is vulnerable to attack. Second, an unauthorized user may be able to access the OA System from a remote location, and thus evade the physical and procedural controls that have been set up to protect the OA System locally.

7.5.2 Hardware/Software Controls

Most current OA System architectures do not provide the hardware features which are needed to implement separate address spaces (or "domains") for the operating system and applications programs. They also do not provide the privileged instructions that are necessary to prevent applications programs from directly performing security-relevant operations, nor do they provide memory protection features to prevent unauthorized access to sensitive parts of the system[16, 21,23].

The limitations of these single-state OA Systems prevent them from providing effective hardware/ software security features. For example, a knowledgeable user can access any memory location directly by using assembly language-type commands. (The memory locations which he/she can access in this manner include not only the system's own semiconductor memory, but also everything currently accessible to any part of the system, such as floppy disks, fixed disks, and cassette tapes.) In this manner, a user can read, modify, and/or destroy any information contained in the OA System--including security critical entities such as password files and encryption information. **The system cannot protect itself from an unauthorized user.**

There are currently a number of hardware and software packages available on the market that claim to provide security for data resident on the system. On all current OA Systems that support only a single processor state, it is easy to circumvent these packages. For example, a user may be able to bypass a security package by booting the system with a different copy of the operating system--one that does not have the security features on it [16,21]. A user may additionally be able to use one of the commercially-available utilities packages to bypass security controls [16,21].

Despite their weaknesses, some current hardware/software packages do have uses. Packages which provide such mechanisms as user identification and authentication, discretionary access controls, and audit trails can provide a degree of protection that is certainly better than that provided by an OA System without them. In addition, hardware/software controls can help to prevent accidents. If these controls are used, it is much less likely that a non-malicious user of the OA System will accidentally gain access to, modify, or delete information belonging to other users. A user will have to make a determined effort to gain access to information belonging to other users.

There are currently some microprocessors available that provide the hardware features necessary to support hardware/software security controls (e. g., multiple processor states). OA Systems that are based on these microprocessors and that have the necessary security mechanisms can be evaluated against the TCSEC [2]. With the proper hardware/software security features added on, it is possible for the OA System to reach the class B1 level, when evaluated against the TCSEC. In addition, if OA Systems are designed with hardware/software security as an initial consideration, they would be able to achieve any trust level defined by the TCSEC.

In summary, hardware/software controls should not be relied upon by themselves to provide separation of users from information in most current OA Systems. However, as long as these controls do not lull the user into a false sense of security, they will not harm and may assist in raising the overall level of Office Automation security.

7.6 Magnetic Media

7.6.1 Magnetic Remanence: Threats, Vulnerabilities, and Controls

Magnetic remanence is the residue remaining on magnetic storage media after a file has been overwritten or the media have been degaussed. Many times, after a file has been overwritten or media have been degaussed, it is still possible for someone with physical possession of the media to recover the information that was formerly present. This magnetic remanence, therefore, is a major vulnerability of any OA System employing magnetic storage media. The threat corresponding to this vulnerability is that persons may come into possession of magnetic media which contain classified or sensitive, but unclassified, information for which they are not authorized. The general control to combat this is for all magnetic media to be properly cleared or declassified before being released for reuse. The following sections give general guidance in the areas of clearing and declassifying magnetic storage media. For more detailed guidance, please see the Department of Defense Magnetic Remanence Security Guideline [4].

7.6.2 Clearing and Declassification of Magnetic Media

Clearing of magnetic media refers to a procedure by which the classified information recorded on the media is removed, but the totality of declassification is lacking. Clearing is a procedure used when magnetic media will remain within the physical protection of the facility in which it was previously used. Declassification refers to a procedure by which all classified information recorded on magnetic media can be totally removed. Declassification is required when magnetic media which have ever contained classified data are to be released outside of a controlled environment.

7.6.2.1 Clearing of Magnetic Media

Certain types of removable media (e.g., magnetic tapes, floppy disks, cassettes, and magnetic cards) may be cleared by overwriting the entire media one time with any one character. Floppy disks may be cleared by applying a vendor's formatting program that overwrites each location with a given character.

Fixed media (e.g., Winchester disks) should be cleared by overwriting at least one time with any one character. One way to do this is by applying a vendor-supplied formatting program that overwrites each location on the disk with a given character, if it can be shown that this program actually works as advertised. The user should beware: some programs that purport to overwrite all locations do not actually do this.

Cleared media may be reused within the controlled facility or released for destruction; however, they should be marked and controlled at the level of the most restrictive sensitivity of information ever recorded.

7.6.2.2 Declassification of Magnetic Media

Certain types of removable media can be declassified using a degaussing device that has been approved for declassifying media of that type. (A list of approved devices is maintained by NSA.)

If a fixed medium (for example, a hard, or Winchester, disk) is operative, an approved method of declassifying the disk pack is to employ an overwrite procedure which must overwrite all addressable locations at least three times by writing any character, then its complement (e.g., binary ones and binary zeros) alternately.

When fixed media become inoperative, it is impossible to declassify the media by the overwrite method. In this case, there are two alternate procedures that may be used: (1) disassemble the disk pack, and degauss each platter with the appropriate approved degaussing equipment; and (2) courier the inoperative media to the vendor's facility, have the magnetic media (e.g., disk platters) removed in sight of the courier and returned to the courier for destruction at the secure site. The vendor can then install new platters and repair any other problems with the disk unit. See Reference 4 for a detailed discussion of each of these alternatives.

7.6.3 Destruction of Magnetic Media

Magnetic media that have contained classified or sensitive, but unclassified, information and are no longer useful should be destroyed. Prior to destruction, all labels or other markings that are indicative of classified or other sensitive, but unclassified, use should be removed.

Detailed methods for destruction of different types of magnetic media are given in Reference 4.

7.6.4 Media Encryption

Cryptography has important applications in an Office Automation environment, since in many cases it is impossible to physically protect magnetic media from all individuals who lack either the clearance or need-to-know for all information contained on the media [22]. (For example, if an OA System with fixed media is shared by two or more users, there quite often is information for which one user does not have a need-to-know that needs to be stored in the system.) In these cases, the use of cryptography to help prevent compromise of classified or sensitive, but unclassified, information should be considered.

In many cases, information security can be enhanced if the information is stored on the media in encrypted form. There are two strategies which can be used: bulk file encryption and integral file encryption. Each of these strategies has its advantages and disadvantages; see Reference 23 for a description of each.

7.7 Environmental Considerations

Office Automation Systems are generally designed to be used in the "typical" office environment [23]. Therefore, they seldom require special environmental controls such as air conditioning or air contamination controls. However, an OA System and its media can be seriously damaged or even destroyed by such things as electrical urges, fire, water, crumbs of food, termites, chemicals, or dust. Since destruction of the system and/or information represents a serious loss to the organization, it is imperative that steps be taken to help prevent unnecessary damage to the OA System. The following discussion is adapted from NBS Special Publication 500–120, Reference 23.

7.7.1 Electrical Power Quality

Surges in electrical power can cause a great deal of damage to an OA System, and can cause information stored within to be permanently inaccessible. Furthermore, frequent power outages cause the loss of use of the system and its resources. Therefore, if the local power supply quality is unusually poor (e.g., large fluctuations in voltage or frequency, voltage spikes, or frequent outages), then such devices as surge protectors, battery backup, or uninterruptible power supply systems should be considered. In addition, disconnecting the system should be considered during intense electrical storms.

7.7.2 Air Contaminants

The general cleanliness of the area in which OA Systems are operated has an effect on reliability, both of the equipment and of the magnetic storage media. Although it is generally not necessary to install special-purpose air purifiers for the OA System, cutting down or eliminating such contaminants as smoke and dust can only help the OA System and its media. The best guidance that can be given in this area is to keep smoke, dust, cigar and cigarette ashes, and similar airborne contaminants as far away from the OA System as possible.

7.7.3 Fire Damage

Fire and excess heat can cause the destruction of an OA System in a very short time. Therefore, any Office Automation equipment in the office should be kept as far away from any open flames or other heat sources as possible. In addition to this, all users of the system should be familiar with procedures to be followed in case a fire should break out. Fire protection equipment (e.g., extinguishers) should be present and conveniently located so that the damage caused by a fire is limited as much as possible [5].

7.7.4 Static Electricity

Another way in which Office Automation equipment can be damaged is by static electricity. If the climate in a particular area results in the presence of large amounts of static electricity, the use of antistatic sprays, carpets or pads should be considered. In addition, since static electricity can quite often build up in personnel, particularly when carpeting is used, personnel can be instructed to discharge any built-up static charge by simply touching a grounded object, such as a metal desk or doorknob.

7.7.5 Other Environmental Considerations

There are other ways in which Office Automation equipment can be damaged by environmental hazards. One of these is by the spillage of food or liquid onto the equipment or media. Spilling a soft drink on a keyboard, for example, can cause damage that requires extensive repair or replacement of the keyboard. Spilling water or crumbs of food onto a floppy disk can cause it to be unusable, possibly resulting in the loss of information stored on it. Therefore, keep all food and drinks away from Office Automation equipment and media [5].

7.8 Preparing Downgraded Extracts

In some instances, it is operationally necessary to copy information from a volume of media at one sensitivity level to another volume that is at a lower sensitivity level. If the OA System does not meet the requirements of at least Class B1, this is always dangerous, as classified or sensitive, but unclassified, information could be compromised without the user's knowledge. Therefore, any decision to permit the electronic downgrading of information should be made only after the risks of compromise have been carefully considered. The person or organization making the decision should be willing to accept the risk that classified or other sensitive, but unclassified, information will be compromised.

Each ADPSSO is responsible for enforcing the procedures by which downgrading of information can be done. The ADPSSO may also be responsible for developing these procedures; however, they may be dictated by organizational policy. The following method is appropriate in some instances; however, the reader should again be warned that the possibility of information compromise exists when this is done:

(l) Format a new volume of media; make sure that it has never been written on before. It would be best if the volume could be removed from a sealed container (e.g., a new box of diskettes).

(2) Copy the necessary information from its current location to the new media.

(3) Carefully examine the new media. Look for any signs that information other than what was intended has been copied. If it is feasible, print out everything on the target media, to verify that they contain no other information.

Of course, it is still possible that information could have been copied onto the new media without being detected. However, if it is necessary that downgrading be permitted, this is a risk that must be taken.

PART IV:

GUIDANCE FOR OTHERS

8.0 RESPONSIBILITIES OF THE ORGANIZATION OWNING* THE OA SYSTEM

Good Information Security begins at the top levels of an organization. If the organization has a commitment to Information Security, there is a far better chance of a security program succeeding. In order to foster good Office Automation System Security, and in turn good Information Security, the following conditions should exist within the organization (e.g., Department, Agency) that "owns" the OA system.

(1) The organization should have a comprehensive Information Security policy. Further, the organization should have an AIS Security policy that ensures the implementation of its Information Security policy for information contained within or processed by AIS. In addition, the organization should have an OA System Security policy that is consistent with both its overall Information Security policy and its AIS Security policy [5]. This OA System Security policy should describe, at a minimum:

(a) What actions are permissible on an Office Automation System, what information may be processed when and by whom, and what is prohibited.

(b) What the organization permits regarding the use of government-owned OA Systems offsite (e.g., at home, or while traveling on official business), the use of personally-owned OA Systems to do government work, and the use of government-owned resources to do outside work (e.g., schoolwork).

(c) Procedures for maintenance of OA Systems.

(d) Procedures for the proper secure operation of an OA System.

(e) Procedures for the secure handling, marking, storage, and disposal of classified or sensitive, but unclassified, information handled by an OA System.

(2) The owning organization should set up a training program to properly instruct users and security officers in the areas of information security, including computer security and Office Automation security. If each person that uses the OA System is properly trained in the security aspects as well as the functional aspects of the system, the chance of a security problem occurring because of user error is significantly decreased.*

(3) The owning organization should have a policy concerning the procurement and use of hardware/software. The organization is responsible for ensuring that all copyrights and license agreements are followed, and that no pirated or otherwise illegally obtained software is used in its OA Systems. Furthermore, the organization should set up a program to test newly purchased or developed software prior to its use in operational systems. The purpose of this program is to ascertain that the software works as advertised, and does not contain trapdoors, Trojan horses, worms, viruses, or other malicious code. (A program of this type is also an excellent way to detect bugs in the software.)

---

*This section applies to any organization responsible for the operation of an OA System, regardless of whether the system is owned, leased, or otherwise obtained.

(4) The owning organization should have a configuration management program that maintains control over changes to the OA System. This program can also maintain records of maintenance done to the system, and keep an inventory of hardware and software to help detect theft [5].

(5) The organization should have a policy covering whether or not audit trails are required and what information is required to be recorded.

(6) The organization should have a policy covering the certification and accreditation of OA Systems that handle classified or sensitive, but unclassified, information [9].

9.0 REQUIRING SECURITY IN THE PROCUREMENT OF OFFICE AUTOMATION SYSTEMS

Security is an important consideration throughout the entire lifecycle of an Office Automation System. If security is not considered during the initial system specifications and Request for Proposal (RFP), it may not be designed into the OA System, and will remain a problem throughout the system life-cycle. Often, when deciding upon what OA System to buy, security is ignored in favor of performance and compatibility with other AIS. Security does not have to be incompatible with other goals; therefore, ignoring it because of them is not valid.

OMB Circular A–130 requires that a risk analysis be done by the person or organization responsible for the security of any AIS before procurement of the system is begun [13]. (Risk analyses are also required at other times during the system life-cycle; see Reference 13 for further guidance.) This requirement applies as much to OA Systems as to any other AIS.

This risk analysis, which may be anything from a very informal review to a fully quantified risk analysis, should help identify potential security problems. These problems can then be addressed before and during the procurement of the system.

(Note: At this point, it is helpful to remind procurement officers and security officers that the prospective vendor’s security claims should be verified to the greatest extent possible. Many times, mechanisms or features claimed by vendors are either not present, or are so easily subvertible that they are of little use.)

The following guidelines should be considered when writing system specifications and Requests for Proposal.

9.1 Processing Classified Information: Policy Requirements

If the OA System will be processing classified information, it must comply with the appropriate national TEMPEST policy directive [13, 14]. The Request for Proposal must state that the system is to meet this policy. Furthermore, if in addition to processing classified information the OA System is to have a communications capability, then appropriate Communications Security (COMSEC) measures, as approved by the National Security Agency, must be taken. The RFP and the system specification should require the capability to adapt to whatever COMSEC measures will be used to protect the system's communications (e. g., compatibility with cryptographic devices).

9.2 Physical Environment of the OA system

An OA System is generally considered to be a high-dollar asset. If the OA System will be kept in an area that does not provide an adequate level of protection against theft, then the purchase of devices that lock the system to a table or in a closet should be considered. Also, the use of OA Systems with the capability for removable-media-only may be considered if there is a high probability of vandalism to the system. If a system with fixed media were to be vandalized, the information stored on the fixed media since the last backup could also be lost, while information contained on removable media can be protected by locking up the media. The probability of vandalism cannot be appreciably lowered by this method, but the damage caused by a vandal can be significantly lessened by protecting the information.

If the OA System will be used to process classified information, and will be kept in an area that is not approved for open storage of information of that sensitivity, an OA System with removable-media-only should be used. This will lessen the chance of compromise of information if an unauthorized user were able to access the system, as classified or sensitive, but unclassified, information could be removed from the system and secured when the system is unattended.

A GSA-approved, tamper-resistant cabinet in which the entire system can be secured should be purchased if the system will be used to process classified information, will contain fixed media, and will be kept in an area that is not approved for open storage of classified information. Given this scenario, this cabinet is the only way in which the security requirements of the system can be satisfied.

9.3 Identification of Non-Volatile Components

All components of the proposed OA System that are non-volatile (i.e., that retain information after power has been removed) should be identified prior to procurement. If the OA System is identified as having only removable media, and there is non-volatile memory that has not been identified as such, then the OA System has been incorrectly identified, since it contains a type of fixed media.

9.4 System Communications Capabilities

If it is known at the time of procurement that the OA System is to be connected with other OA Systems to form a Local Area Network (LAN) then the security requirements of the entire LAN must be considered first. If the procurement is to be of the entire LAN (i.e., of all of its components), then the issues in this chapter must be addressed for the LAN as a whole, as well as for each of its components. Individual nodes of the LAN may have different security requirements than other nodes on the LAN.

If the procurement is to be for an OA System which is to be attached to an existing LAN, then the security requirements and mechanisms of the existing LAN must be examined prior to writing the specifications of the OA System. The new OA System should support all security mechanisms that already exist in the LAN, and should not allow a violation of the LAN's security policy.

(Note: The LAN should enforce a security policy, as any AIS should. This particular security policy should be driven by the owning organization's overall Information Security Policy, and the particular environment in which it operates. See Chapter 8.0 of this guideline for a further discussion of security policies.)

If the OA System must be alternately connected as a terminal to several different AIS that process different sensitivity levels of information, the procurement should specify that only OA Systems using removable-media-only shall be considered. Since the sensitivity level of an OA System with fixed media cannot be easily lowered, switching between AIS with different sensitivity levels of information is impractical, if not impossible, for these systems.

9.5 Shared-Use Systems and Multi-User Systems

A "shared-use system" is an OA System that is used by more than one person, but not by more than one at a time. A "multi-user system" is an OA System that can be used by more than one person at a time. Whenever an OA System is to be shared by more than one person, either serially or simultaneously, there are security concerns which should be addressed that do not occur if the OA System is used exclusively by one person.

9.5.1 Shared-Use Systems Processing One Sensitivity Level of Information

If the system is to be shared by several users, and not all users will have the necessary clearances and need-to-know for all information that will ever be processed or controlled by that OA System, the possibility of acquiring an OA System that uses removable-media-only should be investigated. With this type of system, information can be removed and locked away to prevent its compromise.

If a system with fixed media is procured and used, any information that is stored on fixed media may be accessible to all users of the system. If some users of the OA System do not have a need-to-know for some of the information stored on it, this access is contrary to the provisions of the Privacy Act of 1974 [20] (See Section 3, paragraph (b) of Reference 20). Therefore, if a system that contains fixed media is to be used in this situation, it should meet the requirements of at least class C2, when evaluated against the TCSEC.

9.5.2 Shared-Use Systems Processing Information of Multiple Sensitivity Levels

In many cases, it is desirable to send machine-readable copies of information processed on one OA System to another site for use (e.g., copy a file from one OA System onto a floppy disk, and then use that floppy disk in another OA System). If this is the case, and if the OA System will be used to process several different sensitivity levels of information (e.g., Unclassified through TOP SECRET; personnel, medical, and financial), an OA System that uses removable-media-only should be used. An OA System with fixed media should not be used, since the sensitivity level of the system may not be lowered, and since any removable media which is inserted into an OA System with fixed media must be regarded as having the same sensitivity level as the system itself.

9.5.3 Shared-Use Systems and Multi-User Systems With Fixed Media

If the OA System is to utilize fixed media, and it is desired that users with differing clearances and/or need-to-know be able to access the system, hardware/software security should be specified in the RFP. Specifically, if some users of the OA System do not have a clearance and/or a need-to-know for some of the information to be processed on the system, the RFP should follow the guidance given in References 2 and 3. It is possible that no vendor will be able to respond to the RFP, because there are currently no OA Systems available that meet these requirements. If this occurs, the planned mode of operation of the OA System should be revised to reflect the security capabilities of those systems that are available.

9.5.4 Multi-User Systems Processing Information of Multiple Sensitivity Levels

If it is desired that the OA System be able to simultaneously process and store information of different sensitivity levels, and the system must be trusted to maintain the separation of information by sensitivity level, the specifications should require a system that meets the recommendations given in References 2 and 3. If no vendor is able to respond to the RFP because of lack of hardware/software security controls, the planned mode of operation of the OA System should be revised to reflect the security capabilities of those systems that are available.

10.0 SECURE DISPOSAL OF OFFICE AUTOMATION SYSTEMS

When an Office Automation System has outlived its usefulness and has become obsolete, or when it has become damaged beyond repair, it must be disposed of properly. If the OA System has been used to process or store classified or sensitive, but unclassified, information, certain precautions should be taken before the system can be disposed of through normal channels. These precautions will help to prevent the compromise of any classified or sensitive, but unclassified, information remaining in the system after it is beyond the control of the organization that once used it.

10.1 Removable Media

Any removable media that were used in the OA System should be removed. If these media will be used in another OA System without being cleared, care must be taken to ensure that the new OA System is approved for processing information of the removable media’s sensitivity level.

If it is desired that the removable media be reused in the same facility (but after information currently stored on them is erased), they may be cleared by one of the methods detailed in Reference 4.

In all other cases, removable media that once contained classified or sensitive, but unclassified, information should be either declassified or destroyed, as appropriate, using the methods detailed in Reference 4.

10.2 Fixed Media

Fixed media attached to the OA System that contain or formerly contained classified or sensitive, but unclassified, information should be declassified, destroyed, or removed from the system before they leave the controlling organization. Declassification and destruction procedures are described in Reference 4.

10.3 The Remainder of the OA system

Once both fixed and removable media have been removed from the system and handled appropriately, any semiconductor memory that remains in the system should be properly declassified. To declassify semiconductor memory, the following procedures should be followed prior to disconnecting the power supply. A random pattern of bits must be written over each location. No further data is to be inserted for a 24-hour period and the power is to remain on. This same overwrite procedure should be used a second and third time, i.e., inserting a random pattern of bits and leaving the system powered up for 24 hours, for a total of 72 hours, and no interim insertion of bits. Upon completion of the third cycle, the memory will be considered unclassified. As a second option, the security officer may have the semiconductor memory removed from the OA system and destroyed before the system leaves his control.

Users who cannot use either of these options should contact their organization's Computer Security Office. Additional information is also available from NSA, Ft. George G. Meade, MD 20755–6000, ATTN: Division of Computer Security Standards.

APPENDIX

A Guideline on sensitivity Marking of the Office Automation System and Its Storage Media

Throughout this guideline, sensitivity marking of OA Systems processing classified or sensitive, but unclassified, information and of magnetic storage media is discussed. This appendix provides guidance on how to mark the OA System and its media appropriately.

A.1 Sensitivity Marking of OA Systems Having Removable-Media-Only

The OA System and its peripheral devices must be clearly marked with the highest sensitivity of information that it is allowed to process [9,22]. Stickers indicating the highest sensitivity of information that may be processed by that device should be applied directly to the OA System and each peripheral device. Under normal circumstances, this label should not be removed from the system.

An OA System with removable media (and with only volatile semiconductor memory) is considered to have the same sensitivity level as the media which are currently contained in it. Since OA Systems that do not contain fixed media can change sensitivities (see Section 4.1.2.2), it is recommended that there be a clearly-visible sign placed near the system that indicates when the OA System is being used to process a specific type or range of information (e.g., classified, personnel privileged, proprietary). In this manner, others in the office can be forewarned not to allow visitors to wander about in the vicinity of the OA System. (The user should be aware that this sign might also have the effect of “advertising” the fact that classified or sensitive, but unclassified, information is being processed. This could draw unwanted attention from curious people. Again, the user should be very careful that no one is looking at what is being done.)

A.2 Sensitivity Marking of OA Systems Containing Fixed Media

Any OA System on which classified or sensitive, but unclassified, information is stored is considered to be a sensitive OA System. Any sensitive OA System is assumed to have the same sensitivity level as the highest classified or most sensitive information stored on it. This includes systems with fixed media, as well as systems with nonvolatile semiconductor memory. These systems must always be given the same level of protection as any other information of that sensitivity level [22].

There should be attached to the OA System and each peripheral device, which is not physically collocated with it, a human-readable label (e.g., a sticker) on which is clearly and legibly written the sensitivity of the OA System. Under normal circumstances, this label should never be removed. If the sensitivity level of the system or device changes, a new label indicating the new sensitivity of the system can be placed on top of the old one.

Because of the presence of the fixed media, the sensitivity level of the OA System may never be decreased, unless the system is declassified in accordance with Reference 4.

The label attached to a peripheral device (e.g., a laser printer) that is shared among several OA

Systems should indicate the highest (most restrictive) sensitivity of information that may be sent to that device.

A.3 Sensitivity Marking of Removable Storage Media

The sensitivity level of a volume of removable media is the same as the most restrictive sensitivity level of information stored on that volume. All information on a volume of removable media should be regarded as being at the same sensitivity level (e.g., it is not permissible to consider one file on a diskette to be TOP SECRET and another file on the same diskette to be Unclassified).

There should be a human-readable label attached to the container of each volume of removable media (e.g., the outside of a diskette, the outside of a tape reel) that clearly indicates the current sensitivity level of that volume of media [5,1l,12,22,23]. Under normal circumstances, this label should not be removed unless the volume of media is declassified using procedures specified in Reference 4. Labels should be color coded in accordance with applicable government and agency or departmental standards.

> Example: An orange label may be used to indicate a TOP SECRET diskette, a red label indicates a SECRET diskette, a blue label indicates CONFIDENTIAL, a purple label means personnel data is contained on the diskette, a grey label indicates "Company X Proprietary Information," a green label may be used on a diskette that contains unsensitive information only.

The volume of media should then be protected to a level that is at least commensurate with this label.

> Example: A floppy disk that is marked SECRET should be given the same level of protection as a piece of paper that is marked SECRET (e.g., stored in a GSA-approved safe when not in use).

It is permissible to raise the sensitivity level of a volume of media. When this happens, the label on the media should also be changed. A new label indicating the higher sensitivity level may be placed on top of the old label, or the old label may be removed before the new label is applied.

It should not be permissible to decrease the sensitivity level of a volume of media without first declassifying it using one of the approved methods described in Reference 4.

Any volume of media which is in the OA System at the same time as other media of a more restrictive sensitivity level should automatically acquire that more restrictive sensitivity [l6].

> Example: If an Unclassified system disk is placed in drive A of an OA System, with a TOP SECRET disk in drive B, the system disk should be considered to be TOP SECRET and protected as such. The reason for this is that the average user has no way of being absolutely certain what is being written on each disk, and must therefore guard against the OA System writing to the wrong disk by upgrading the sensitivity of the system disk.

Any volume of removable media that is not sealed in its original package and is not labeled should be presumed to be at the same sensitivity level as the OA System in which it is used [5,l5]. If this OA System can have a range of sensitivity levels (e.g., is a system with removable-media-only), the volume of media should be considered to have the same sensitivity level as the highest classified or most sensitive information the system can process.

If there is an unsealed, unlabeled volume of media, and it cannot be determined which (if any) OA System it has been used in, the media should be considered to have the same sensitivity level as the highest sensitivity level of any OA System that they could have been used in.

> Example: Suppose that there are four OA Systems in the same room. Three are Unclassified systems, while the fourth is TOP SECRET. An unlabeled floppy disk is found lying on top of a desk in this room, and it cannot be determined in which, if any, of these four OA Systems this particular floppy has been used. This floppy disk should therefore be considered to be TOP SECRET.

A.4 Sensitivity Marking of Fixed Storage Media

All fixed media should be regarded as having the same sensitivity level as the OA Systems to which they are attached.

Unless the OA System has been approved to simultaneously process information of a range of sensitivity levels, all information on the fixed media should be regarded as being at the same level: the highest sensitivity level of any information on the media.

LIST OF ACRONYMS

ACRONYM	EXPANSION
ADPSSO	ADP System Security Officer
AIS	Automated Information System
LAN	Local Area Network
NACSI	National Communications Security Instruction
NCSC	National Computer Security Center
OA System	Office Automation System
PC	Personal Computer
TCSEC	Department of Defense Trusted Computer System Evaluation Criteria
WP	Word Processor

GLOSSARY

ADP System Security Officer (ADPSSO)

The person who is nominally responsible for the secure operation of an OA system.

Automated Information System (AIS)

An assembly of computer hardware, software, and firmware configured in such a way that it can collect, communicate, compute, process, disseminate, and/or control data.

Connected Office Automation System

An OA System that is electrically connected to one or more AIS. The OA System may be used as a host, a file server, a terminal, or any other component of a network.

Local Area Network

An interconnected group of OA Systems or system components that are physically located within a small geographic area, such as a building or campus.

Magnetic Remanence

A measure of the magnetic flux density remaining after removal of an applied magnetic force. Can also mean any data remaining on ADP storage media after removal of the power.

Multi-User System

An OA System that can be used by more than one person simultaneously.

Non-removable Magnetic Media

Any magnetic media used for the storage of information that is not designed to be regularly removed from the system. Examples of non-removable media include fixed or “Winchester” disks. (This will also be referred to as “fixed media'' for short.)

Nonvolatile Memory

Memory contained within an Office Automation System that retains its information after power has been removed.

Office Automation System

Any microprocessor-based AIS or AIS component that is commonly used in an office environment. This includes, but is not limited to, Personal Computers, Word Processors, printers, and file servers. It does not include electric typewriters, photocopiers, and facsimile machines.

Personal computer (PC)

A microprocessor-based computer which is primarily intended to be used by one person at a time. It is usually characterized by relatively low cost and small physical size (usually small enough to fit on a desk or table).

Physically Protected Communications Media

Any communications media to which physical access is sufficiently controlled that the chance of compromise, improper modification, or destruction of information is assumed to be zero.

Removable Magnetic Media

Any magnetic media used for the storage of information that is designed to be frequently and easily removed from the Office Automation System by a user. Examples of removable magnetic media include floppy disks, removable hard disks (e.g., Bernoulli disks) and magnetic tapes. (This will also be referred to as "removable media" for short.)

Sensitive, but Unclassified Information

Information the disclosure, loss, misuse, alteration, or destruction of which could adversely affect national security or other Federal Government interests. National security interests are those unclassified matters that relate to the national defense or the foreign relations of the U.S. Government. Other government interests are those related, but not limited to the wide range of government or government-derived economic, human, financial, industrial, agricultural, technological, and law enforcement information, as well as the privacy or confidentiality of personal or commercial proprietary information provided to the U.S. Government by its citizens [19].

Sensitivity Label

The physical representation of the sensitivity level of information.

Sensitivity Level

A designation, associated with information, indicating (l) the amount of harm that can be caused by the exposure of that information to an unauthorized user, (2) any formal access approvals that must be granted prior to the granting of access to that information, and (3) any specific handling restrictions placed on that information. Sensitivity levels contain both a hierarchical component (e.g., Unclassified, CONFIDENTIAL, SECRET, TOP SECRET) and a non-hierarchical component (e.g., For Official Use Only (FOUO), Proprietary Information Enclosed (PROPIN)).

Shared-Use System

An OA System that is used by more than one person, but is used by only one person at a time.

Stand-Alone Office Automation System

An OA System that is electrically and physically isolated from all other AIS.

Volatile Memory

Memory contained within an Office Automation System that loses its information a short time after power has been removed.

Word Processor (WP)

An Office Automation System that is designed to be used primarily in the preparation of documents containing alphanumeric text.

Workstation

The total collection of Office Automation equipment, physically located in one place, that makes up the resources meant to be used by one person at a time.

REFERENCES

1. U.S. Air Force Computer Security Program Office, "Guidance for Secure Operating Procedures for the Zenith Z–l50 Personal Computer," 1 June 1985.

2. Department of Defense Standard 5200. 28–STD, "Department of Defense Trusted Computer System Evaluation Criteria," 26 December 1985.

   (Note: this document is also referenced as: DoD Computer Security Center, Department of Defense Trusted Computer System Evaluation Criteria, CSC–STD–001–83, 15 August 1983.)

3. DoD Computer Security Center, Computer Security Requirements--Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments, CSC–STD–003–85, 25 June 1985.

4. DoD Computer Security Center, Department of Defense Magnetic Remanence Security Guideline, CSC–STD–005–85, 15 November 1985 (FOR OFFICIAL USE ONLY).

5. Department of Energy, "Security Guidelines for Microcomputers and Word Processors," DOE/MA–0181, March 1985.

6. Executive Order 12356, National Security Information, 6 April 1982.

7. Federal Emergency Management Agency, "Information Systems Policy," Instruction 1500.3, 23 March 1984.

8. Federal Emergency Management Agency Manual 1540.2, "Automated Information Systems (AIS) Security," September 1984.

9. Federal Information Processing Standards Publication (FIPS PUB) 102, Guideline for Computer Security Certification and Accreditation, 27 September 1983.

10. Department of the Interior, "Acquisition and Use of Microcomputers," 376 DM 12.1.

11. Lawrence Livermore National Laboratory, "Computer Security Guidelines for Microcomputer Users," January 1985.

12. Los Alamos National Laboratory, "Word Processor Security Policy," June 1982.

13. Office of Management and Budget (OMB) Circular A–130, "Management of Federal Information Resources," 12 December 1985.

14. National COMSEC Instruction (NACSI) 5004, "TEMPEST Countermeasures for Facilities

Within the United States (U)," l January 1984 (SECRET).

15. National COMSEC Instruction (NACSI) 5005, "TEMPEST Countermeasures for Facilities Outside of the United States (U)," 1 January 1984 (SECRET).

16. National Computer Security Center, Personal Computer Security Considerations, NCSC–WA–002–85, December 1985.

17. National Security Decision Directive 145, National Policy on Telecommunications and Automated Information Systems Security, September 17, 1984.

18. National Telecommunications and Information Systems Security Policy (NTISSP) No. 2, "National Policy on Protection of Sensitive, but Unclassified Information in Federal Government Telecommunications and Automated Information Systems", 29 October 1986.

19. U.S. Nuclear Regulatory Commission, NRC Manual, Chapter NRC–2301, "Systems Security", March 16, 1985.

20. Public Law 93–579, "Privacy Act of 1974," 31 December, 1974.

21. Schaefer, Marvin, "Security Vulnerabilities of Office Automation Systems," in Proceedings of the Security Affairs Support Association's Fall 1985 Symposium: "INFOSEC FOR THE NINETIES", 21–22 November 1985.

22. Department of State, "Security Standards for Office Automation Systems used for National Security Information in the Washington, D.C. Metropolitan Area," A/ISS Systems Security Standard Number 1, 22 December 1985.

23. Steinauer, Dennis D., Security of Personal Computer Systems: A Management Guide, NBS Special Publication #500–120, January 1985.

DISTRIBUTION:

NSA
NSC (ATTN: Mr. DeGraffenreid)
OMB (Intel Branch NSD)
ODASD (C^3I) (Greg O'Hara) (2)
OJCS (C3S) (2)
CSA (DAIM–OI) (2)
CSA (DAMI–CIC) (2)
CSA (DALO–SMC) (2)
CSA (DAMA–CSC) (2)
CNO (OP–941) (3)
CMC (CC) (5)
USCINCCENT (RC6J6–O) (2)
USCINCEUR (C3S) (2)
USCINCLANT (C3S) (2)
USCINCPAC (C3S) (2)
USCINCRED (RCC4S–O) (2)
USCINCSO (J6) (2)
HQ USAF (SITT) (3)
HQ SPACECMD (2)
HQ MAC (SI) (2)
HQ SAC (SI) (2)
HQ TAC (SI) (2)
AFCSC (EPXP) (20)
AFCSC/EPVL
COMUSFORCARIB (J6) (2)
COMUSFJAPAN (J6) (2)
COMUSFKOREA (J6) (2)
DIR ARFCOS (2)
DCSO (CODE B210) (20)
DIA (RSI–5) (10)
DIS (V0410) (5)
DLA (DLA–TI) (2)
DNA (LECD)
DIR TRI–TAC (TT–SC)
CDR JTE/JTC3A
CDR USAINSCOM (IAOPS–OP–P) (15)
CDR USACSLA (SELCL–NMP) (5)
COMNAVSECGRU (G–61) (15)
COMDT COGARD (GTES–5)
COMCOGARDLANTAREA
COMCOGARDPACAREA
COMCOGARDONE

COMCOGARDTWO
COMCOGARDTHREE
COMCOGARDFIVE
COMCOGARDSEVEN
COMCOGARDEIGHT
COMCOGARDNINE
COMCOGARDELEVEN
COMCOGARDTWELVE
COMCOGARDTHIRTEEN
COMCOGARDFOURTEEN
COMCOGARDSEVENTEEN
COMNAVELEXSYSCOM (PDE 110–231) (3)
DCMS (T60) (6)
CG MCDEC (DEVCEN C3) (2)
Dept. of Agriculture (MSD/FAS) (2)
Dept. of Commerce (IS) (2)
Dept. of Energy (CSTM (2)
Dept. of Health & Human Services (IG) (2)
Dept. of Interior (AMO) (2)
Dept. of Justice (JMD/SS) (2)
Dept. of State (ASC) (2)
Dept. of Transportation (OIS M–50) (2)
Dept. of Treasury (AIT) (10)
CIA (OC–CSD) (2)
CIA (DIR OIT) (2)
CIA (OS MAIL) (ATTN: CHARLES U.) (2)
CIA (Chief, TEMPEST Division, OS) (2)
DIR, IC STAFF (IIHC) (2)
DIR, IC STAFF (DCI SECURITY COMMITTEE) (2)
DIR, IC STAFF (POLICY AND PLANNING STAFF) (2)
DCA (Code B310)
DMA OTS (OMD)
DMA TT
Drug Enforcement Administration (AIOC) (2)
FAA (ADL–15) (6)
FBI (TSD) (5)
FCC (OMD) (2)
FEMA (OP–IR) (7)
GSA (KJS) (6)
NASA (NIS) (20
NASA (TS) (15)
NCS (MGR) (2)
NRC (5721–NMBB) (2)