



**UNITED STATES AGENCY FOR  
INTERNATIONAL DEVELOPMENT**

---

**AUTOMATION  
SECURITY  
GUIDEBOOK**

AGENCY FOR INTERNATIONAL DEVELOPMENT  
OFFICE OF INFORMATION RESOURCES MANAGEMENT  
AUTOMATION SECURITY GUIDEBOOK

APRIL 15, 1988

AGENCY FOR INTERNATIONAL DEVELOPMENT  
OFFICE OF INFORMATION RESOURCES MANAGEMENT  
AUTOMATION SECURITY GUIDEBOOK

TABLE OF CONTENTS

<u>TITLE</u>	<u>PAGE</u>
INTRODUCTION .....	1
A. GENERAL INFORMATION SYSTEM SECURITY RESPONSIBILITIES .....	2
A.1 MANAGEMENT RESPONSIBILITIES .....	2
A.2 OPERATIONAL RESPONSIBILITIES .....	3
A.3 USER RESPONSIBILITIES .....	6
A.4. MISSION ACCOUNTING AND CONTROL SYSTEM (MACS) RESPONSIBILITIES.....	7
B. PHYSICAL SECURITY .....	8
B.1 SECURITY OF OPERATIONAL ENVIRONMENT .....	8
B.2 SECURITY OF MAGNETIC MEDIA .....	9
B.3 ENVIRONMENTAL CONTROLS .....	10
B.4 EMERGENCY SHUTDOWN OF SYSTEM .....	11
C. SYSTEM SECURITY .....	12
C.1 GENERAL SECURITY REQUIREMENTS .....	12
C.2 WANG VS SECURITY FEATURES .....	13
C.3 OFFICE INFORMATION SYSTEMS (OIS) SECURITY REQUIREMENTS .....	18
C.4 TELECOMMUNICATIONS SECURITY .....	19

AGENCY FOR INTERNATIONAL DEVELOPMENT  
OFFICE OF INFORMATION RESOURCES MANAGEMENT  
AUTOMATION SECURITY GUIDEBOOK  
TABLE OF CONTENTS - CONT'D

<u>TITLE</u>	<u>PAGE</u>
D. MICROCOMPUTER SECURITY .....	21
D.1 MICROCOMPUTER VULNERABILITY .....	21
D.2 MICROCOMPUTER SECURITY REQUIREMENTS .....	21
D.3 PROCESSING OF LOU/CLASSIFIED INFORMATION ON MICROCOMPUTERS .....	22
D.4 PERSONALLY-OWNED MICROCOMPUTERS .....	22
E. ADMINISTRATIVE/PROCEDURAL SECURITY .....	24
E.1 ADMINISTRATIVE CONTROLS .....	24
E.2 PCs AS WORKSTATIONS/ ARCHIVING WORKSTATIONS .....	27
E.3 EXTENDED OPERATIONS .....	27
E.4 PROCESSING OF LIMITED OFFICIAL USE (LOU) MATERIAL .....	27
F. RISK ANALYSIS/CONTINGENCY PLANNING .....	30
F.1 RISK ANALYSIS .....	30
F.2 CONTINGENCY PLANNING .....	31

AGENCY FOR INTERNATIONAL DEVELOPMENT  
OFFICE OF INFORMATION RESOURCES MANAGEMENT  
AUTOMATION SECURITY GUIDEBOOK  
TABLE OF CONTENTS - CONT'D

<u>TITLE</u>	<u>PAGE</u>
G. COMMON SENSE SECURITY MEASURES .....	33
G.1 ADMINISTRATIVE SECURITY .....	33
G.2 PHYSICAL SECURITY .....	34
G.3 MICROCOMPUTER PROTECTION .....	35
G.4 SOFTWARE SECURITY .....	35
G.5 PERSONNEL VULNERABILITIES.....	36
G.6 CONTINGENCY PLANNING .....	37
G.7 COMMON DON'TS .....	37
H. GLOSSARY OF TERMS .....	38

APPENDICES

A. LOG PROCEDURES .....	A-1
B. SYSTEMS SECURITY OFFICER (SSO) CHECKLIST	B-1
C. SAMPLE LOGON PROCEDURES .....	C-1
D. BIBLIOGRAPHY .....	D-1

ATTACHMENTS

1. A.I.D./W Notice from IG/SEC: Processing LOU Materials on WP and OIS Equipment in A.I.D./W (April 3, 1987) .....	1-1
2. Federal Information Resources Management Regulations (FIRMR) Bulletin 34: Microcomputer Security (December 24, 1985) .....	2-1

AGENCY FOR INTERNATIONAL DEVELOPMENT  
OFFICE OF INFORMATION RESOURCES MANAGEMENT  
AUTOMATION SECURITY GUIDEBOOK  
TABLE OF CONTENTS - CONT'D

<u>TITLE</u>	<u>PAGE</u>
3. OMB Circular Number A-130: Security of Federal Automated Information Systems (December 12, 1965) .....	3-1
4. National Security Decision Directive 145 (NSDD-145): National Policy on Telecommunications and Automated Information Systems Security (September 17, 1984) .	4-1
5. Telegrams:	
1985 State 378130: Processing of LOU Information	
1985 State 337721: LOU Processing	
1987 State 139964: Processing of LOU Information	
1987 State 132298: A.I.D. Information Systems Security Policy .....	5-1

## **INTRODUCTION**

AGENCY FOR INTERNATIONAL DEVELOPMENT  
AUTOMATION SECURITY GUIDEBOOK

INTRODUCTION

The Office of Information Resources Management (M/SER/IRM) plans, develops, procures, and supports all automated systems in the Agency for International Development (A.I.D.). This Security Guidebook, prepared by IRM, sets forth Agency policies and procedures guiding all operating expense funded, unclassified A.I.D./Washington and overseas automated systems. It is designed to serve as a reference for overseas Missions and for Offices and Bureaus in A.I.D./W engaged in automation activities not under the direct control of M/SER/IRM.

A.I.D. recognizes its information resources to be very valuable assets. As such, these resources must be carefully managed and protected from unauthorized access and use.

The developing age of information presents new challenges to managers concerned with computer and information security. The central purpose of this guidebook is to provide A.I.D. personnel, in A.I.D./W and overseas, with guidance in the execution of the Agency's security policies, standards, and procedures in order to:

- . Protect A.I.D.'s proprietary information
- . Prevent damage to A.I.D.'s operational environment from misuse, fraud and theft
- . Protect A.I.D.'s information resources.

These security guidelines were developed primarily for A.I.D.'s WANG VS, OIS, and WP systems, and all microcomputers. The guidelines do not cover the IBM mainframe facility in A.I.D./W.

Where applicable, sections of the guidebook were derived from the Department of State (DOS) System Security Standards for unclassified automated information systems, and from other U.S. Government Documents such as OMB Circular A-130 and NSDD-145. A complete list of sources is attached as Appendix D.

Policies and informational material contained herein are subject to modification and updates which will be issued as developments within A.I.D. and information systems technology warrant.

NOTE: Questions concerning these guidelines should be referred to the Director, Office of Information Resources (M/SER/IRM), with a copy to the Inspector General, Office of Security (IG/SEC).

## A. GENERAL INFORMATION SYSTEM SECURITY RESPONSIBILITIES

### A.1 MANAGEMENT RESPONSIBILITIES

The intent of this section is to define and address the responsibilities of Agency personnel charged with carrying out A.I.D. automation security policies. It is recognized that conditions differ at installations and that one individual may hold more than one designation or that duties may be delegated beyond those defined here.

#### Mission, Bureau and Office Directors

It is Agency policy that Mission, Bureau and Office Directors are responsible for the technical and physical security of all information systems hardware and software under their jurisdiction. The following security personnel generally are delegated to assist in security oversight of an organization's information system:

#### Regional, Post and Unit Security Officers

At overseas posts, the Department of State Regional Security Officer (RSO), and/or Post and Unit Security Officers, according to local conditions, assist and advise principal officers in discharging overall security responsibilities. The general duties of the RSO, Post, and Unit Security Officers are defined in A.I.D. Handbook 6, Sections 990.3 through 991.2.

At A.I.D./Washington, a Principal Unit Security Officer is designated by the head of each major functional area to assist in carrying out the area's overall security responsibilities. The general duties of the Principal Unit Security Officer are defined in A.I.D. Handbook 6, Sections 992 through 992.2.

In both the overseas and the domestic environment, the role of the Regional, Post and Unit Security Officers in information security is to cooperate with and assist management and responsible information systems personnel in:

- . Discovery of incidents bearing on systems security
- . Coordinating investigations of systems security incidents
- . Protecting automated data processing (ADP) data, reports, equipment, and sites
- . Advising where to get help when an actual or suspected security problem is discovered
- . Performing risk analyses and contingency planning.

## A.2 OPERATIONAL RESPONSIBILITIES

Operational responsibility for the security of the organization's information resources rests on the following personnel:

### Systems Security Officer (SSO)

At overseas posts, it is A.I.D. policy that an American direct-hire employee will serve as the Mission's Systems Security Officer (SSO). Therefore, each Mission with an unclassified automated information system will designate an American employee to be the SSO for managing and implementing the automated information system security program described in this guidebook. The following criteria will be used:

- . At Missions where A.I.D. automation systems are physically part of an Embassy automation system managed by a Department of State Information Systems Security Officer (ISSO), the A.I.D. system will also be under the supervision of the State ISSO.
- . At locations where A.I.D. is independent, the A.I.D. American Systems Manager will be designated SSO.
- . At locations where there is no American Systems Manager at the Mission, the Mission must designate an American employee, preferably one with knowledge of automated systems, to perform the system security function.

At A.I.D./Washington, Bureaus/Offices will designate appropriate direct-hire personnel to implement these automated information system security policies and procedures.

Both overseas and at A.I.D./Washington, the primary responsibility of the SSO is to assure that automated information systems are installed and operated in a manner consistent with these security standards.

In both areas the SSO has specific security duties, including to:

- . Disseminate these standards and other appropriate guidance on automated systems to all users.
- . Cause system operations to be suspended, partially or completely, if so justified by the suspected systems compromise.

- . Browse word processing documents periodically to ensure that classified information or other material that should not be widely disseminated, such as sensitive medical or personnel records, is not resident on the system.
- . Report events which may constitute security violations or system penetration attempts to the appropriate A.I.D. officer, and to IRM and IG/SEC (and the RSO, if overseas) if the Principal Officer determines such action to be warranted.
- . Conduct periodic compliance surveys and security evaluation reviews and keep a record of the results.
- . Monitor the issuance and control of all user IDs and passwords.
- . Coordinate with the personnel office to establish procedures to promptly notify the SSO of changes in the status of employees, such as termination or transfer, in order that the SSO can take appropriate action regarding system access by those employees.
- . Provide appropriate systems security training, as well as periodic security briefing to all persons with access to the automated system.
- . Conduct risk analyses and develop appropriate contingency plans for the automated information system environment. (see Section F)
- . Develop additional security procedures to supplement these standards as needed for local operating conditions.

**NOTE:** Whenever State's ISSO addresses any A.I.D. system security activities, a copy of the report will be sent to IG/SEC and M/SER/IRM. The A.I.D. SSO will closely coordinate with the State ISSO and the RSO in all automation security issues.

### **Systems Manager**

The Systems Manager (SM) is responsible for overseeing the day-to-day operations of the automated system at the Mission or at A.I.D./W. As noted above, this individual, if an American direct-hire employee, may also be designated Systems Security Officer. It is recommended that a detailed background check be performed by the RSO for a non-American Systems Manager.

The Systems Manager's security-related duties include:

- . Establishing the software, hardware, and physical security environment.
- . Following the security instructions of the System Security Officer (SSO).
- . Reporting any security-related problems to the SSO.
- . Backing up and restoring data files as needed.
- . Arranging for data storage, both on- and off-site, to protect Agency information.

Under the direction of the SSO, the SM develops the procedures for establishing access to system applications, programs, and data files. Because of the sensitivity of these duties, the SSO must be extremely careful when granting SM authority to any individual.

Once access control procedures have been set up, the SM enters the various data, e.g., user IDs, passwords, data file access limits, etc., necessary for implementation.

Thereafter, the SM keeps the access control data current to provide for changes in personnel assignments, hardware, software, and programs. Depending on the size and activity level of the system, this could require daily changes.

#### Assistant Systems Manager

The Assistant System Manager, if any, will be supervised by the SM and may, under certain circumstances, assume the responsibilities and duties of the Systems Manager in his/her absence. His/her duties include:

- . Assisting the Systems Manager in the performance of his/her daily operational functions.
- . Following the security instructions of the Systems Manager and Systems Security Officer.
- . Reporting to the SM and/or the SSO any abnormal system operation.

**NOTE:** The SSO may also grant SM authority to the Assistant Systems Manager to assure that an individual with SM access is always available. The number of SMS will be kept at the minimum consistent with need.

### A.3 USER RESPONSIBILITY

Users of information technology systems must also accept responsibility for security of these systems by:

- . Monitoring access to workstations located in their work areas.
- . Reporting any abnormal conditions which affect security to the SSO or SM.
- . Logging off terminals when not actually using them.
- . Protecting passwords by not sharing them or writing them down.
- . Informing the SSO or SM in the event of a known or suspected compromise of a password.
- . For microcomputer (PC) users, safeguarding both hardware and data.
- . Complying with automated information systems security regulations.
- . Controlling disposal of output, including using burn bags, shredders, or other means appropriate to the sensitivity of the material.
- . Ensuring that all information on storage media (tapes and diskettes) is reviewed and, if necessary, erased before allowing the media to be reused.

Employees are reminded that nonofficial use of any A.I.D.-managed automated system is prohibited and could result in disciplinary action.

#### A.4 MISSION ACCOUNTING AND CONTROL SYSTEM (MACS) RESPONSIBILITIES

The Mission Accounting and Control System (MACS) is an Agency automated accounting and financial management system which was developed for use at overseas posts.

A.I.D. Controllers set MACS system access rights and limitations, and establish data handling procedures in accordance with local needs. The central security concerns of MACS are:

- . Data integrity
- . The prevention of unauthorized use of USG and/or other funds
- . Data availability and accuracy.

The Controller maximizes accounting controls by segregating responsibilities and by building appropriate procedural checks and balances into work processes.

The MACS System Administrator has the responsibility to provide data processing and logistical support to MACS users. The duties of the Administrator may be performed by other technical staff, but the Administrator has the ultimate responsibility and should have a good working knowledge of MACS design, procedures and performance. It is recognized that in some Missions the MACS system administrator may, in fact, be the Systems Manager.

The MACS Site Coordinator is the Controller's Office MACS representative. This individual coordinates, directs, and supervises all MACS-oriented accounting transactions. He/she also may act as a liaison between the Financial Management Office, the Data Management Office, and Mission personnel.

The Data Controller receives source documents from other offices and documents generated from within the Controller's Office. He/she classifies these documents by transaction type and logs the document in the appropriate section of the Document Control Log.

## **B. PHYSICAL SECURITY**

This chapter provides guidance on physical security measures needed to safeguard A.I.D. automated systems and the information resident on them. An effective physical security program also introduces internal system controls.

### **B.1 SECURITY OF OPERATIONAL ENVIRONMENT**

#### **B.1.1 Access Controls to the VS/OIS Room**

The room housing the VS or OIS - often referred to as the "Computer Room" or "Information Center" - must be designated a controlled area and be properly secured with a locking device approved by the RSO or IG/SEC. Information Center door combinations must be controlled and changed as necessary and at intervals not to exceed six months.

The number of persons authorized access to the room should be kept to a minimum, with only those persons directly involved with running the system, and security personnel, having unescorted access. The use of the computer room as a work area should be limited to computer operators.

Visitors, such as users and equipment maintenance personnel, should be allowed access to the computer room only when authorized by the SSO or SM, and should be escorted by a person authorized computer room access.

A plan should be in place to allow authorized personnel to enter the area after duty hours in case of fire, flood, power problems, or other threats to the site. Instructions for action to be taken in case of such threats should be readily available to duty officers, security personnel, and others who might have to respond in the absence of systems staff.

#### **B.1.2. Security of Small Information Systems**

Small information systems such as WANG WP, small OIS and VS systems, and microcomputers located in open work areas should be placed so that their use may be easily monitored.

When necessary, room or equipment locks should be used to protect such systems against theft.

### B.1.3 Security of Peripherals (Workstations/Printers)

Peripherals should be located in areas where they can be physically secured and/or monitored by authorized users. If a peripheral is in an area where it cannot be seen by an authorized user (e.g., kept in a small room, out of sight of user), then it should be secured by a locking device on the peripheral or the door of the room.

It is recommended that terminals and printers be physically or logically disconnected after normal business hours, or when they cannot be monitored effectively.

The SSO or SM should maintain a complete inventory of peripherals and their locations as well as a list of individuals responsible for them.

## B.2 SECURITY OF MAGNETIC MEDIA (TAPES AND DISKS)

Magnetic media are like paper documents which contain information that is written on them and therefore are subject to disclosure. In all cases, magnetic media must be protected; demountable magnetic media containing A.I.D. information should be stored in an appropriate security container. Physical access to tapes or disks must be restricted to avoid deliberate or inadvertent removal.

Minicomputer installations often include the tape/disk library and the system in the same room. This has the advantage of requiring only a single controlled access room, but also increases the potential for loss from fire or flood. Where possible, backup data critical to the organization's mission should be stored completely away from the computer room. (For example, a reciprocal arrangement might be reached with the Embassy computer facility for storage of tapes and disks.)

Whenever demountable magnetic media such as tapes or disks are moved, such as to another site, the SM should record their removal and return in an appropriate log.

A degaussing device may be employed when the recording medium is to be reused or disposed of. While the degaussing device should completely remove the previously recorded information, it is possible that traces will remain and the media should be handled accordingly.

### B.3 ENVIRONMENTAL CONTROLS

The automated system's environment is a security concern, because an improper environment can cause severe damage to the system. Consider the following:

- . High temperature and humidity levels can damage electronic circuitry, disks, and magnetic tapes. Air conditioning systems should be provided to maintain equipment at levels recommended by the maker(s). Depending on local conditions, backup air conditioning should be available.
- . The use of recording thermometers and hygrometers will aid in maintaining proper temperature and humidity levels.
- . The automated system should have the "cleanest" power possible; that is, it should if possible be on a dedicated power line. If local power is not dependable or is unstable, consider use of a power conditioner, Uninterruptible Power Supply (UPS), or other means of avoiding power fluctuations that can damage the equipment.
- . Dust and sand infiltration can seriously damage automation equipment. Equipment should be kept in as dust-free an environment as possible. Filters should be changed or cleaned regularly.

#### B.3.1 Construction Standards

M/SER/IRM, with copy to IG/SEC, should be contacted for guidance before moving existing automation installations or constructing new facilities.

Windows and openings in the computer room which are at ground level or which could be accessible to intruders should be protected with metal bars. In general, windows should be avoided or permanently sealed.

The computer room should be located with due regard for security from water damage, strength of weight-bearing floors, ease of meeting temperature and power requirements, and sufficient space to allow for entry, installation, and maintenance of the equipment.

An emergency power-off control should be readily accessible to operating personnel during normal work hours and to security personnel during nonoperational hours. The proper placement for this control would be immediately inside the door to the information center.

The power-off control should disconnect the air conditioning serving the information system equipment room and the power to all electronic equipment in the room except for an emergency light.

### **B.3.2 Water Detection**

Water resulting from burst pipes, accidentally-triggered fire sprinklers and the like can extensively damage automated systems (plastic sheets should be available to cover the equipment in case of emergency). Sensing devices should be placed in the information center to detect water when the room is unattended. These devices can be connected to a master alert system at a guard station, or they can sound an alarm.

### **B.3.3 Fire Protection**

The SSO and/or the SM should ensure that fire sensors are strategically placed in the computer center, and that users practice fire prevention rules. The following types of protective systems may be used:

- . Ionization, light-scattering, and heat detecting smoke and/or fire detectors. These can be part of a master alert system wired to a guard station, or they can sound an alarm.
- . Halon 1211 fire extinguishers, both hand held and ceiling-installed. Halon is an excellent extinguishing agent, but can be dangerous if not used with care. Personnel should be trained in its use and maintenance.

As part of the organization's overall fire plan, every A.I.D. automation facility should have an emergency team prepared to respond to a fire alarm and help to evacuate the building, use fire extinguishers, shut down the system, protect storage cabinets from water, activate fire suppression systems, and, as appropriate, assist the local fire department.

## **B.4 EMERGENCY SHUTDOWN OF SYSTEM**

In cases of general building emergencies - fire, earthquake, mob action, bomb threat, and the like - systems personnel should exercise judgment in powering down equipment and evacuating the area. To avoid uncontrolled access to the system during the emergency, users should be logged off and the system powered down normally if time permits. Otherwise - again, time permitting - use of the emergency power-off control is recommended.

See Section F for a discussion of contingency planning.

## C. SYSTEM SECURITY

This chapter addresses system security standards and procedures for A.I.D. automated information systems, except the IBM mainframe.

### C.1 GENERAL SECURITY REQUIREMENTS

#### C.1.1 Logon User ID

The SM is responsible for establishing logon user IDs and passwords for VS minicomputers and for OIS systems requiring passwords for access. Each user must have his/her own ID and password.

#### C.1.2 Passwords

The SM must assign all users a password to access the system. Passwords should be selected at random and should not be names, nicknames, or initials, or have any obvious significance to their owners.

Variable length passwords may also be used, provided they are within the eight-character maximum permitted by the WANG security system. This means the various users of a system will have different length passwords, making it more difficult for someone to guess a password.

Passwords will be assigned only on the basis of need to access the system. A written request from the password applicant's supervisor requesting access and defining access needs should be required before assigning a password.

In the event a user forgets his/her password, the SM will assign a new password to reduce the possibility of compromise.

The assigning of group passwords is NOT allowed. Each password must be assigned to one person only.

Passwords should be changed at regular intervals. A shorter time interval provides better security. The recommended time between password changes is three months.

The SM should control the addition and deletion of users or revision of access rights. Passwords should be changed and new passwords issued (or deleted, if appropriate):

- . Immediately following any suspected security compromise

- . When an individual is no longer employed with the Agency
- . When it is determined that an individual no longer requires access to the system
- . When the user moves from one office or section to another
- . At least every 3 months.

All users must be made aware of the confidential nature of a personal password. It is the responsibility of the SSO to inform the user that disclosure of a password is not authorized. It is the responsibility of the user to inform the SSO if such disclosure is suspected or occurs.

Customer Service Engineers may be issued a logon ID and password only when required to perform service. The password should be changed upon completion of the service call.

## C.2 WANG VS SECURITY FEATURES

The WANG VS contains a comprehensive security system which allows the System Security Officer to protect information resources against unauthorized use.

The VS Security System allows the SM to:

- . Add or remove users
- . Define user system access privileges
- . Review, modify, or delete user system access privileges
- . Define file protection classes unique to the installation
- . Define and modify program access privileges and priorities
- . Review, modify, or delete intersystem access privileges
- . Maintain full control over the resources of the VS Security System.

The following features of VS Security can be defined for individual users through the SECURITY program (see Chapter 2 of the WANG VS System Administrator's Reference and Chapter 4 of the VS System Administrator's Learning Guide for a complete discussion):

## **File Protection Classes and Access Privileges**

When created, every program and data file is assigned to a specified file protection class. SSOs and SMs should develop assignments of file protection classes for various user groups or applications based on the examples and information provided in the above-mentioned VS System Administrator manuals.

Although usage constants (default locations of files, file protection class for output files, etc.) may be set through the Command Processor by the user, logon procedures should be used to set default values (see Section C.2.2 below).

### **Owner-of-Record File Class Control**

It is possible for a user to create a file in a class for which that user does not have access privileges. As the owner-of-record of the file, that user has full access to the file, even if the owner is not authorized access to other files of that class. This awkward situation cannot be prevented through normal, available system procedures. However, two means are available to help ensure that files are assigned to the proper file protection class:

- . Publish a list of file categories for all personnel to use when creating files
- . Establish logon procedures for each system user containing a SET statement that specifies a default file protection class for all files created by that user. (See Section C.2.2 for logon procedures.)

### **Workstation Logon Restrictions**

Users, except those identified by the SSO as requiring general workstation access, should have their ability to logon to the system restricted to or from a limited number of workstations in order to inhibit users from accessing information on terminals outside their area.

### **Help Key**

In order to provide flexibility to users, the Help Key on A.I.D.-controlled unclassified automated systems will generally not be disabled.

## **VS System Security Administrator**

The VS System Security Administrator (SSA) has access to all files on the system, including the SECURITY program and all private files. Under normal circumstances, only the SSO and the SM would have these privileges.

### **Operator Privileges**

Operator privileges should be assigned only to the System Manager and authorized system operators. They should be assigned based on logon ID. Only the system console should have dual-mode privileges.

### **Program Access Rights**

The special access privileges given to a program are not passed on to the user running the program. Only the SSO or his/her designee, e.g. an applications programmer, can change a program's access privileges. This method of granting access privileges to a program instead of to a user should be used for all programs on the system.

#### **C.2.1 The SECURITY Utility**

The SECURITY utility protects information resources at the system, file and access levels:

At the system level, the LOGON process restricts access to users whose profiles are in the system User List. (Refer to WANG'S VS System Administrator's Reference for information on assigning LOGON privileges.)

At the file level, users may access only those files belonging to the file protection class or classes to which they have been granted access rights. Access to other files is denied by the system. Up to 30 unique file protection classes can be defined. Programs can also be granted these access rights.

At the access level, for each file protection class accessible by a user, different access privileges can be specified so that some files can be modified, some can only be read and executed, and some program files can only be executed. The same categories of access privileges can also be assigned to a program independently of its current user.

SSOs and SMs should carefully consider the previously described system security features when assigning user access privileges through the SECURITY program.

## System User List

The data file USERLIST is created by the SECURITY program. It contains the IDs, names, and access rights of all designated system users. This file is located in library @SYSTEM@, on the system volume. To help ensure that users work only in assigned libraries and applications, the SM and the SSO should print out and review the system user list monthly.

The file USERLIST should have a # protection class.

### C.2.2 Logon Procedures

To aid in controlling user access to the system, logon procedures should be established and assigned to all users according to their need. A logon procedure is typically used to do two things:

- . It can set any usage constants (workstation defaults) that the user would otherwise have to set through PF2 from the Command Processor menu (Set Usage Constants). For example, the procedure could set the print class and print mode to be used for print files created by the user.
- . It can either run a specific program or display a menu of program options for the user. A logon procedure for a word processing operator might simply run the word processing software. A logon procedure for a data entry clerk might display a menu with options for accessing several different data entry programs.

For more information on Logon Procedures, see Chapter 4 of the WANG VS System Administrator's Learning Guide and the VS Procedure Language Reference. A sample logon procedure is included in Appendix C.

### C.2.3 PROTECT Command

The PROTECT Command allows a job's or library's protection class to be modified. When a file is created, the ID of the creator is recorded in the file label, and the user becomes the owner of the record. The owner of a file can be changed with the PROTECT command.

Once a file is assigned to a file class, only the owner and users with access rights to that file can obtain access to the file. In addition, only the owner and the SSO can use the PROTECT command to reassign a file to another class.

Refer to the WANG VS System Administrator's Reference, Chapter 2, for more information on how to use the PROTECT Command.

#### C.2.4 Additional VS Security Measures

The following files in @SYSTEM@ should be protected by a pound sign (#) to restrict their use to the SM and designated SSAs:

- . BACKUP
- . COPYWP
- . DISKINIT
- . LISTVTOC
- . USERLIST
- . WPCNCFG
- . WPCNFGM
- . WPCRCVS
- . WPSDUPD
- . WPSDUPDL
- . WPSDUPDM
- . WPSDRCCM
- . WPSDRCSM
- . WPSDRVC
- . WPSLIBC
- . WPSLIBCM
- . WPSMAKL
- . WPSMAKLM
- . WPSPWCH
- . WPSPWCHM
- . WPSRUNPP

The SECURITY program should be renamed to prevent user access to the SECURITY program.

Any USERAIDS installed on the system should be reviewed and, if necessary, restricted to appropriate users. (USERAID PASSWORD, for example, allows users to change their own password.)

#### Running Applications or Programs from Word Processing

The run program or procedure capability through word processing will be restricted to individuals authorized by the SSO.

## Controlled User Environment (CUE)

CUE is a software security system developed by the Department of State for use at State minicomputer installations. Since A.I.D. uses the security measures noted in this document, CUE is not used on minicomputers owned by the Agency. Any exception to this must be approved by M/SER/IRM.

### C.3 OFFICE INFORMATION SYSTEMS (OIS) SECURITY REQUIREMENTS

#### C.3.1 General Requirements

Missions and A.I.D./W offices with a WANG OIS will, like VS installations, designate an SSO and an SM. These individuals are responsible for maintaining an appropriate level of security on the system. The SM has additional responsibility for the following OIS-related functions:

- . The SM should ensure that a password is assigned to Supervisory Functions during initial software installation.
- . The SM should conduct a spot check of all libraries weekly to ensure that documents containing A.I.D. information that should not be widely distributed are being regularly archived by their owners.
- . The SM should periodically print each volume catalog to identify files (excluding documents) that have been added or deleted since the previous printing.
- . The SSO and SM should utilize the OIS Peruse Log List feature regularly to review the users who are currently logged on to the system. The information provided on the Log List is the user ID, the system name, the unit number, the user's class, and the logon status. Regular use of the OIS Peruse Log List will help ensure that users work only in assigned libraries and applications.

#### C.3.2 Logon and Passwords

OIS Security is an optional software package supported by OIS systems 40, 50, 60, and 100 Series. It is recommended that this option be installed on Agency OIS systems. (See WANG'S OIS Systems Administrator's Guide, Chapter 2, for information on installing OIS Security.)

The SM will follow the same procedures described earlier in this chapter for generating, disseminating, and maintaining user logon IDs and passwords.

In addition, the following requirements with respect to passwords apply to OIS:

- . Passwords for access to supervisory functions should be changed quarterly by reloading the supervisory software diskette(s).
- . Volume passwords should be changed each time the operating system is upgraded or the system software is reinstalled.
- . If a user finds the need to password a document, the document should be archived or erased from the system as soon as possible.

### **C.3.3 Word Processing System Security Requirements**

The predecessors of the OIS are the stand-alone word processing systems such as the WANG WPS 5. Generally most stand-alone word processing systems currently used in the Agency provide few system-based security controls. The WANG WPS 20, 25, and 30 have a security option that enables users to protect documents by assigning write protection and read protection passwords.

## **C.4 TELECOMMUNICATIONS SECURITY**

### **C.4.1 International Communications System (ICS) - Connectivity to Department of State Systems**

The International Communications System (ICS) provides for interchange of documents and data between A.I.D. overseas Missions and A.I.D./W, using the A.I.D./W main computer as central switch and mailbox.

The use of the communications facility is restricted to unclassified documents and data only. No classified or LOU material will be transmitted via this network. Overseas posts and Regional Bureaus should coordinate what documents can be transmitted via ICS.

The system makes use of leased lines provided to A.I.D. by the Department of State, as well as dial-up communications for those posts not yet supported by the DOS telecommunications network.

Use of DOS communications capability does not imply connection to DOS processors, even though such processors may physically share a multiplexor or link. Under the definition of connectivity in DOS System Security Standard Number 5, ICS usage of DOS lines does not constitute connectivity. Therefore, the regulations of DOS System Security Standard Number 5 do not apply to the A.I.D. systems originating the ICS links.

Any questions regarding specific system connectivity to DOS computers should be addressed to M/SER/IRM.

## D. MICROCOMPUTER SECURITY

Microcomputers are able to perform a wide range of functions including statistical analysis, spread sheets, economic analysis, project tracking, graphic displays and word processing. These systems are usually configured with hard disks, thereby increasing their ability to store data on line. Optionally, WANG microcomputers can serve as fully functional workstations on a VS or OIS system giving them file access and data manipulation capability. Whenever a microcomputer is configured as a workstation, access to the system must be controlled by A.I.D.'s security access control procedures.

This section addresses A.I.D.'s security guidelines regarding the use of microcomputers to process data both on and off A.I.D.-controlled premises.

### D.1 MICROCOMPUTER VULNERABILITY

Although elaborate security measures can be employed to protect mainframe computers, microcomputers afford almost unlimited opportunity for intrusion into the unit itself.

- . Data can be modified and no record of the change can be found.
- . It is very easy to remove the whole machine.
- . Access to data is not easily controlled.
- . Users may not maintain adequate documentation and backups of programs and data.

### D.2 MICROCOMPUTER SECURITY REQUIREMENTS

Following are security practices that should be employed to protect microcomputer hardware and software. The SSO and SM should ensure that this information is included in user training programs.

- . Users must be aware of their responsibility to protect their data and equipment, including the necessity for making periodic backups of program files and data.
- . Data files containing information that should be protected should not be identifiable by name. A separate printed index of the files can be maintained in a locked and secured area.

- . Floppy disks containing data should not be left in the open. Store floppies in a safe place.
- . Locks must be used to protect information resources at all times. For example, microcomputers left in open office areas should be physically secured to a desk or wall.
- . Removable hard disk options which have been evaluated and approved by IRM may be considered for storing information that should be controlled.
- . The only sure way to destroy a diskette is to physically cut it into pieces.
- . Only hardware/software approved by IRM should be used.
- . Microcomputers removed from A.I.D. premises should be subject to standard property pass procedures (see Section E.1.1)

#### D.3 PROCESSING OF LOU/CLASSIFIED INFORMATION ON MICROCOMPUTERS

Processing of LOU/Classified information on microcomputers is subject to the regulations and restrictions cited in section E.4

#### D.4 PERSONALLY-OWNED MICROCOMPUTERS

Personally-owned microcomputers are used at many A.I.D. posts and in Washington. Individuals frequently move data and text back and forth between office-based equipment and equipment at home so that they can work evenings and weekends. Similarly, some employees use personally-owned portable microcomputers to assist them while on TDY or while visiting project sites away from the U.S.A.I.D. Data and text used during such TDYs often are transferred to the Mission's systems when the traveler returns.

To avoid inhibiting the productivity of employees after hours or on TDY, A.I.D. policy authorizes employees to use personally-owned microcomputers for business purposes provided:

- . Neither classified nor LOU information is processed on the equipment
- . Reasonable precautions are taken to avoid the misuse of information that should not be widely distributed

- . Systems are not developed for internal A.I.D. use through hardware or software that is inconsistent with A.I.D.'s equipment/systems standards.

Any exception to the policy must be approved by M/SER/IRM.  
(reference State 132298, May 1, 1987)

## E. ADMINISTRATIVE/PROCEDURAL SECURITY

### E.1 ADMINISTRATIVE CONTROLS

Administrative security involves establishing operational and accountability procedures that provide acceptable protection for information resident on automated information systems. Administrative security measures provide managers with control of the workflow within a system. They ensure that work passes only from one responsible element to another and that information is not stolen or modified.

The following section discusses the human element and the application of management and supervisory controls over the use of information resources including:

- . Data processing
- . Storage media
- . Systems and application development
- . Telecommunications.

Administrative security controls involves the supervision and ability of management to detect and correct security abuses.

Administrative Security procedures include:

- . Dividing functions and duties based on the employee's need to know.
- . Tailoring access controls to ensure that data and files are available only to authorized personnel.

Access controls are determined by:

- . The type of work to be performed
- . The time access is required
- . The location from which the data will be accessed - remote, or local terminal, or microcomputer
- . How the data will be used
- . Who will use the information.

### **E.1.1 Log and Record Keeping**

At a minimum, the following logs and records should be maintained by the SSO and/or SM:

#### **Loan or Removal of Automation Equipment from A.I.D. Premises**

These guidelines apply to all A.I.D. automated systems and their hardware components, such as circuit boards, keyboards, disk packs, tapes, modems, etc.

- At A.I.D./Washington, removal of U.S. Government-owned property from A.I.D. premises is controlled through the use of nonexpendable property passes (see Handbook 20, Section 7G.4).
- At A.I.D. Missions overseas, movement of nonexpendable property should be controlled in accordance with established Mission procedures. It is recommended that a system similar to the property passes issued in Washington be used.

**System User List** - A list to be maintained by the SSO of all persons authorized system access. It should contain name, organization, user ID, access level, and the date the user was added to and/or deleted from the system. The SSO or SM will periodically review access levels, particularly for sensitive applications, with the user's supervisor.

**Operations Area Access List** - A list to be defined and maintained by the SSO of all persons who have unescorted access privileges to sensitive areas relating to the automated information system. This should include remote tape and disk storage areas as well as the central computer facility.

**Visitor Log** - It is recommended that a record be kept of all visitors who require escorted access to the locked facility.

**After-Hours Use Log** - A record of requests for system use outside of normal work hours (see section E.3)

### E.1.2 System Maintenance Procedures

The SM should be notified before maintenance personnel or other vendor service personnel are allowed to access a system. Maintenance personnel will be closely and continuously supervised during the maintenance period.

Any magnetic media, circuit boards or other equipment brought into or removed from the systems facility should be logged and monitored by the SM.

Certain WANG diagnostics allow for the reading, display, and modification of data on magnetic storage devices mounted on the system. Care must be taken to prohibit maintenance personnel from using diagnostics or other methods to randomly browse through data or documents stored on the system.

As stated earlier, passwords issued to Customer Service Engineers should be changed at the end of each service call.

**System Operations Log** - A log should be kept of all normal daily operations, including the use of all magnetic storage media, that lists media used, dates and time of use, and user ID. The log should also list all problems reported, services performed on the system by date, time, service performed, circuit boards replaced or removed for service, and system or application software installed or removed (See Appendix A).

### E.1.3 IDs for Visitors

When approved by the SSO, the SM may assign temporary system access IDs to TDY visitors at the written request of the visitor's control officer. The request should include the effective dates of access validity. These requests should be retained to provide a log of temporary IDs issued.

The temporary IDs should permit minimum access to perform the required activities. This can be controlled through appropriate logon procedures.

The SSO and/or SM should periodically review the user list and delete all expired visitor IDs.

## E.2 PCs AS WORKSTATIONS/ARCHIVING WORKSTATIONS

A WANG personal computer, when used as a workstation, qualifies as an archiving workstation. Access to the system by these workstations must be controlled through the VS security system. Data and documents may be transferred between the PC and the VS in accordance with the user's VS access privileges.

Archiving workstations should be located where they can be monitored by authorized personnel or else locked in a room to which only authorized users have access. As with all unclassified automated equipment, an unclassified archiving workstation must never be used to produce, copy, or print classified documents.

The SSO should know the location of each archiving workstation and the individuals with authorized access.

## E.3 EXTENDED OPERATIONS

If the computer facility is in operation beyond business hours, the following minimum standards will be followed:

- . The system must not be used after hours unless an authorized member of the systems staff is present. The SM must be notified by the intended user when the system is needed for after-hours use.
- . All after-hours usage will be noted in a log maintained by the Systems Manager and submitted to the SSO for periodic review.
- . System maintenance personnel are prohibited access to the computer facility after normal business hours unless escorted by an authorized employee.

## E.4 PROCESSING OF CLASSIFIED AND LIMITED OFFICIAL USE (LOU) MATERIAL

CONFIDENTIAL, SECRET, AND TOP SECRET MATERIAL WILL NOT BE PREPARED, PROCESSED OR STORED ON NON-TEMPEST INFORMATION SYSTEMS.

Per 5 FAM 958.1 (A.I.D. Handbook 6), LOU material is defined as "certain sensitive information and material which is not national security information and therefore, is not classifiable but nevertheless warrants a degree of protection."

In A.I.D./Washington, employees may process LOU material on non-TEMPEST information systems provided the following conditions are met:

- . All LOU documents processed on non-TEMPEST information systems equipment must be password protected. If the equipment does not have the capability for placing a password on LOU documents, it may not be used for processing LOU material.
- . All tapes and floppy diskettes which are used for the storage of LOU material shall be secured (security container) at the close of each working day (para. 958.1, 5 FAM 900).

At overseas Missions, the processing of LOU material is dependent upon the Mission's classification as a high or low technical threat post:

- . Missions in high technical threat Foreign Service posts must ensure that LOU information is not processed and/or stored on a non-TEMPEST system. Questions concerning high technical threat posts should be addressed to the RSO, SSO, or IG/SEC/PSI.
- . Missions at other than high technical threat posts may process LOU on non-TEMPEST approved information systems where access is restricted to cleared American citizens and FSNs with LOU clearances. This is best suited to personal computers and small OIS systems (e.g., OIS 60 and below).
- . The "Security Erase" feature is used to delete LOU information from systems with nonremovable disks (e.g., OIS 60 and PCs with Winchester Drives).
- . Systems having a removable and a nonremovable disk must be secured by disabling the nonremovable portion when the system is used for LOU processing.
- . All tapes and floppy diskettes which are used for the storage of LOU material shall be secured in a security container at the close of each working day (para. 958.1, 5 FAM 900). No magnetic media containing LOU information will be left on the system unattended for any reason.
- . Missions must not send systems with nonremovable disks approved for the processing of LOU information outside of the Mission for maintenance.

It is the responsibility of the Systems Security Officer to approve, in writing, the use of an unclassified system for LOU processing and ensure that all of the above criteria are met.

(References: 1985 State 337721, 1987 State 139964)

## F. RISK ANALYSIS/CONTINGENCY PLANNING

Performance of risk analysis and development of a contingency plan for the automated information resources, especially at an overseas Mission, is one of the most important tasks of the Systems Security Officer. Both the analysis and the plan should take into account the overall emergency plans of the Mission (or A.I.D./W), and as such, should be coordinated with the Regional, Post, or Unit Security Officer.

### F.1 RISK ANALYSIS

The SSO and SM should conduct a thorough study of the automated environment to determine what risks would be faced in case of an emergency. This can be done by:

- . Determining what threats are likely to occur and their consequences.
- . Determining the value of each information resource that is threatened and compare that with the cost of protecting it.
- . Identifying and prioritizing the activities and resources that are most important to the operation.

These tasks will form the basis for the development of a contingency plan. Before proceeding with any of the above steps, the threats that are likely to occur must be identified and discussed in a scenario so that an effective response can be developed to protect or recover the resources involved.

Threats to be considered should cover all possible disasters: fire, water damage (caused by broken pipes, flood, rain), sandstorms, earthquake, explosion, lightning, electrical power failure, heating and air conditioning failure, vandalism, terrorist attacks, human errors, and hardware/software failure.

The value of a resource may not necessarily be monetary, but may also include information critical to the operation or programs of the Agency. Replacement costs should take into consideration not only hardware costs, but also time and personnel involvement to recoup losses.

## F.2 CONTINGENCY PLANNING

Once the risk analysis has been performed, the SSO should develop a step-by-step contingency plan and recovery process which should be integrated into the overall emergency plan of the Mission. The plan should address various levels of threat or disaster and contain specific actions to be taken in each case.

The planned emergency responses must be documented and roles assigned to responsible individuals to ensure that Agency information and resources are protected and that recovery from disasters achieves complete system operation in as little time as possible.

A modified version of such plans should be included in instructions to the duty officer and local guard force for implementation in the event that an emergency occurs outside of normal work hours.

Contingency plans should be reviewed at least yearly, or when there is a substantial change in the threat situation.

Contingency/recovery plans should address such points as:

- . Backup of critical hardware, software, and data, including backup processing agreements with other agencies or companies having similar facilities. When appropriate, Missions or A.I.D./W may consider off-site storage for their information assets such as disk packs, systems and applications documentation, operating manuals, magnetic tapes and production libraries. Mission information resources may be stored at banks or other secured sites through mutual agreements.
- . Specific responsibilities for executing the plan. As appropriate, specific positions (rather than personnel by name) should be identified to carry out portions of the plans. Backup positions should also be identified.
- . The priority of each activity. Based on time available for response during a given incident, certain activities will become more crucial. For example, it may only be possible to hit the emergency power control switch before evacuating the facility, rather than calmly logging off users and powering off the system.

- . Procedures for notifying key personnel. In case of after hours emergencies, the facility guards should know whom to contact (the SSO and SM) and how they can be reached.

A contingency plan should therefore include:

**What Must Be Done.** The plan must provide as many details as possible about the exact steps to be followed in each of the identified threats or disasters. Include minimum actions to be taken.

**When Must It Be Done.** Establish the proper sequence of each step. If a deadline is required, or if the step is a prerequisite to some other action, specify these requirements clearly.

**Who Must Do It.** Normally, the SSO or SM should be in overall charge of the recovery effort. Each major operation should be assigned to a responsible individual (designated by position), with backups designated.

**How It Should Be Done.** The methods to be followed must be clearly described, especially if nontechnical people are to perform any of the operations. This is important in the modified plan developed for the security force.

**What Is Needed To Do The Job.** Determine the amount of money, people and other resources that must be applied to the task. If specific resources (fire extinguishers, alarm systems, etc.) are required, action should be initiated to procure them. Contingency funds should also be included in the Mission's overall budget.

## G. COMMON SENSE SECURITY MEASURES

Common sense security measures provide basic security without incurring additional hardware or software expenses. Such measures can be very effective in reducing the threat to information resources.

Following are some common sense suggestions that SSOs and SMs should find applicable to most automated information installations.

### G.1 ADMINISTRATIVE SECURITY

- . Publicize information security procedures and policies.
- . Continually monitor Mission automation operations with an eye to potential security risks.
- . Take prompt action in reporting security violations.

#### Password Management

- . Change passwords at least every three months.
- . Encrypt or otherwise protect from unauthorized access the computer-stored password file.
- . Do not use a common password for everyone in an area.
- . Invalidate the passwords of individuals who leave the Office/Mission.
- . Establish and enforce password rules - and be sure everyone knows them.

#### Authorization Procedures

- . Use authorization procedures that identify which users have access to which information.
- . Require supervisors to request authority for an employee to use computer resources, gain authorization to specific information and applications, and receive a password.

## File Protection

- . In addition to a user identification and authorization policy, develop procedures to restrict access to data files.
- . Use external and internal file labels to identify the type of information contained and the required security level.
- . Restrict access to areas that contain data, such as off-site backup facilities, on-site libraries, and off-line files.
- . Use software, hardware, and procedural controls to restrict access to files to authorized users.

## G.2 PHYSICAL SECURITY

- . Care must be exercised when disposing of reports or documents. They often supply easy access to material in offices where printed reports are the main form of backups.
- . Store and lock disks, tapes and other operational records when not in use.
- . Use a filing system to keep track of disks and tapes.
- . Don't lend storage media to unauthorized persons.
- . Return damaged or defective disks to vendors only after degaussing or use of a similar procedure.
- . Dispose of disks, diskettes, and tapes by degaussing, shredding, or other means of destruction.
- . Dispose of printouts and printer ribbons in accordance with Agency security procedures.
- . Secure printouts of passwords and other access information.
- . Power surges can erase memory, alter programs, and destroy microcircuits. Consider purchase of an Uninterruptible Power Supply: a device which allows enough time to shut down a computer without losing data. Prevent momentary power surges from damaging computers by using voltage regulators. In a thunderstorm, unprotected small computers should be turned off and unplugged.

- . Excessive heat can be controlled by air-conditioning systems and fans, and by ensuring that air can circulate freely. A common problem is stacking peripheral equipment or blocking air vents on terminals or small computers.
- . Air filters can remove the airborne contaminants that harm equipment and disks. Ban smoking near computers.
- . Locate automation equipment away from potential water hazards, such as plumbing pipes, areas known to flood, or even sprinkler systems if other fire protection devices are available.
- . Keep food, beverages, and ashtrays away from the equipment.
- . Keep equipment in good working order. Monitor and record hardware maintenance. This provides both an audit trail of persons who have had access to the system and a record of contract fulfillment. Maintenance personnel must carry proper identification.

### G.3 MICROCOMPUTER PROTECTION

- . Guard microcomputers from power surges through voltage regulators, power conditioners, or battery packs.
- . Prevent theft with locks.
- . Make sure users backup information and store copies in a safe place.

### G.4 SOFTWARE SECURITY

- . Restrict access to libraries containing programs and files to authorized personnel.
- . Periodically work with users to spot-check programs to verify they are processing as designed.
- . Review reports produced by the programs for unauthorized output. Report distribution should be restricted to personnel with a need to know.
- . Fully implement the operating system's security features.

- . Terminate jobs for which security violations have been detected and hold for action by the SSO.
- . Properly maintain applications documentation.
- . Establish procedures for monitoring program changes.

#### G.5 PERSONNEL VULNERABILITIES

The following are examples of personnel vulnerabilities which may require defensive action:

- . Terminated or transferred employees are not prevented access to the automated system.
- . Employees are unaware of information security concerns and the need to protect information.
- . Unauthorized computer products, such as computer art, games, sports, and betting pools, appear in the work area.
- . The same technical employees work in all phases of the system--data entry, data analysis, and data output.
- . Unscheduled programs are run on a recurring basis, particularly during hours of low computer usage.
- . The level of background clearance required by employees has not been considered.
- . Users do not take information security vulnerabilities very seriously; they assume that security problems will not occur at their site.
- . Employees have little motivation and low morale. Relationships with management are poor.
- . There is evidence of unusual employee behavior or problems, such as gambling, alcoholism, or drug abuse.
- . Employees who are seldom absent from the office and who often choose to be secluded from other employees may be engaging in unauthorized systems use.

## G.6 CONTINGENCY PLANNING

- . Include automated information facility contingency plans in the Mission's, bureau's, or office's emergency plan.
- . Consider both natural and man-made threats when making contingency plans.
- . Make sure the local guard force and duty officer are aware of emergency plans for the facility.
- . Connect alarm systems to a central guard station.

## G.7 COMMON DON'TS

- . Don't share passwords with anyone.
- . Don't write passwords on desks, walls, or terminals--commit them to memory.
- . Don't leave the workstation logged on and unattended.
- . Don't use the computer for personal business.
- . Don't have automated information in only one place--back it up.
- . Don't forget to secure printouts containing information which should not be widely disseminated.
- . Don't copy licensed software packages and don't use copies someone else has made.
- . Don't assume that an automated system is always protected. Plan for contingencies.
- . Don't assume information security just happens. Do your part.
- . Don't go it alone. Seek help when you need it.

## H. GLOSSARY OF TERMS

**Access.** The ability and the means necessary to approach, to store, or retrieve data; to communicate with, or to make use of any resource of an ADP system.

**Access Control.** The process of limiting access to the resources of an ADP system only to authorized users, programs, processes, or other ADP systems (in computer networks). Synonymous with controlled access, controlled accessibility.

**Accountability.** The quality or state which enables violations or attempted violations of ADP system security to be traced to individuals who may then be held responsible.

**Administrative Security.** Management operational procedures and controls instituted to protect information and information resources.

**Archiving Workstation** A workstation that has a floppy disk drive onto which information can be copied.

**Assistant Systems Manager.** Performs systems duties under the supervision of the Systems Manager and may assume the responsibilities of the Systems Manager in his/her absence.

**Backup.** The process of copying files from one volume to another to protect them from accidental loss.

**Communications.** Transmitting data by means of a computer network system; also, telecommunications.

**Customer Service Engineer.** Generally an employee of the equipment vendor, the "CE" performs routine system maintenance and tests, as well as diagnosing and repairing hardware problems.

**Contingency Planning.** Program to minimize disruption caused to an organization in case of loss of its automation technology resources.

**CPU.** The computer's central processing unit.

**CUE.** Controlled User Environment. A security software system developed by the Department of State.

**Data Storage Media.** Floppy diskettes, magnetic tapes, and hard disks.

**Degauss.** To apply an alternating current (AC) field for the purpose of demagnetizing magnetic recording media, and thereby erasing any information contained thereon.

**Encryption.** Protecting information by encoding it through use of appropriate encryption/decryption keys.

**Environment.** The aggregate of external circumstances, conditions, and events that affect the development, operation, and maintenance of a system.

**FIPS Pubs.** Federal Information Processing Standards Publications.

**Fire Walls.** Walls that have been sufficiently fireproofed to prevent the spread of fires.

**Floppy Disk.** Low-cost mass storage medium consisting of a thin, circular, flexible sheet of Mylar with a magnetic-oxide surface. Sometimes called a diskette.

**Group Access.** Common (shared) file access for a group of users.

**Halon System.** A fire suppression system using Halon gas. Halon is especially suited for computer facilities because it does not damage electronic equipment.

**Hardware.** Tangible aspects of information systems equipment.

**Hardwire.** To physically connect automated technology equipment by means of a cable.

**Host.** A computer that accepts and processes jobs from remote terminals or computers.

**Hot Site.** A backup computer facility to be used in case of shutdown, through accident or otherwise, of a primary computer site.

**Intelligent Terminal.** A data communications terminal with internal data storage and processing capabilities.

**Interactive.** Real time dialogue between terminal and computer.

**ISSO.** Information System Security Officer (the Department of State counterpart to A.I.D.'s SSO).

**LAN.** Local area network. (see Local Network)

**Library.** Collection of software programs or routines.

**Link.** A connection (not necessarily hardwired) for communication.

**Local Network (Local Area Network).** A data communication facility providing high-speed switched connections between processors, peripherals, and terminals within a single building.

**Limited Official Use (LOU).** Certain sensitive official information which is not national security information but which nevertheless requires a degree of protection.

**MACS.** Mission Accounting and Control Systems. The A.I.D. automated accounting system developed for overseas use.

**Mainframe Computers.** Large central-site computers used for the heaviest data processing requirements.

**Magnetic Media.** Devices on which information is recorded in digital form, such as magnetic tapes, diskettes, and hard disks.

**Memory.** The computer's information processing area.

**Microcomputer (PC).** A small, often portable, computer intended for individual use.

**Microprocessor.** A small device usually built on a semiconductor chip that has basic computer capabilities (such as instruction processing, logic, arithmetic, and control).

**Minicomputer.** A small, usually multi-user computer. It has less pure computing capability than a mainframe.

**Modem (Modulator-Demodulator).** A device to receive and transmit information over communication media.

**Networks.** Associated components interconnected for such functions as communications and resource sharing.

**OIS.** WANG'S Office Information System. Designed primarily for word processing, but also supports list processing, BASIC programming language, and limited data processing applications.

**Operating System.** The software furnished by a manufacturer for a computer system to control its mode of operation and interface with users.

**Orange Book.** Department of Defense Trusted Computer System Evaluation Criteria (CSC-STD-001-83, August 15, 1983).

**Password.** A protected word or string of characters that identifies or authenticates a user, specific resource, or access type.

**Physical Security.** The use of locks, guards, badges, and similar administrative measures to control access to the computer and related equipment. The measures required for the protection of the structures housing the computer, related equipment, and their contents from damage by accident, fire, and environmental hazards.

**Read Access.** Ability given to a user to read information contained in the computer system.

**Risk Analysis.** An analysis of system assets and vulnerabilities to establish an expected loss from certain events based on estimated probabilities of the occurrence of those events.

**Sanitize.** The degaussing or overwriting of information in magnetic or other storage media.

**Security Policy.** The rules and practices that regulate how an organization manages, protects, and distributes resources such as information systems.

**System.** An assembly of hardware and software configured for the purpose of processing, transmitting and receiving, storing, and retrieving data.

**Systems Manager (SM).** The individual responsible for the day-to-day operations of the automated system.

**System Users.** Individuals who use the system in the performance of their work.

**System Operator.** An individual, normally on the systems staff, whose job it is to perform the routine operational functions of the automated system.

**Systems Security Officer (SSO).** An American Officer designated to manage information systems security in each Agency element.

**Systems Programmer.** Software developer responsible for design, development, installation, and documentation of the operating system, peripheral utility programs, and modifications.

**Tape Librarian.** Person in charge of filing, retrieving, and accounting for storage media (tapes, disk packs, cartridges).

**Telecommunications.** Communication over relatively large (usually more than a few hundred meters) distances, by microwave, satellite, or hardwired lines.

**Teleprocessing.** Data processing over telecommunication links.

**TEMPEST.** Term used to refer to automated information system components that use approved emanation suppression/containment systems for the processing and storage of classified national security information.

**Terminal.** A data entry device for communicating alphanumeric characters, programs, and commands to computers and similar devices. They may or may not have "intelligence" (the ability to store, modify, or edit data before transmission).

**Uninterruptible Power Supply (UPS).** A system that maintains AC power during a temporary outage by continuing to derive DC power from batteries and converting it to AC power.

**User-Friendly.** A system or program that is easy for users to learn and use.

**Word Processor.** A text preparation device with memory and intelligence, to allow information to be prepared and edited electronically before printing.

**Write Access.** Ability given to a user to write an object or record.



**APPENDIX B**  
**SYSTEMS SECURITY OFFICER (SSO) CHECKLIST**

## APPENDIX B

### SYSTEMS SECURITY OFFICER (SSO) CHECKLIST

As part of his/her responsibilities for ensuring compliance with automation security requirements, the SSO must:

- . Monitor the activities of any employee with access to system administrator and/or supervisory functions.
- . Cause operations to be suspended, partially or completely, as soon as possible after detecting actions which appear to jeopardize the security of the automated information system.
- . Ensure effective implementation of automation security requirements by providing copies of this guidebook as well as appropriate guidance and training on systems security to all system users.
- . Conduct periodic reviews to ensure that systems security measures are understood and actively practiced by systems users.
- . Evaluate, at least semiannually, threats to and vulnerabilities of the organization's automated information system.
- . Report any system failure, attempt to gain unauthorized access, or any other event which might lead to compromise or destruction of A.I.D. information resources to the appropriate management and Security Officer. A copy of the incident report should be provided to M/SER/IRM and IG/SEC.
- . Take appropriate measures to protect all automated information system resources from damage, destruction, alteration, or misappropriation.
- . Generate, issue, control and maintain permanent written records of access authorizations to all personnel allowed access to the automation facility and equipment, to include users, contractors, and maintenance personnel.

## APPENDIX B

### SYSTEMS SECURITY OFFICER (SSO) CHECKLIST - CONT'D.

- . Manage the generation and dissemination of all system and user ID numbers and passwords. Change user passwords at least quarterly in order to reduce the chance that they will be learned and used by unauthorized personnel.
- . Remove users from system access when they no longer have need because of changes in their employment status. Similarly, passwords for the entire group of users must be changed upon the change in status or departure of any employee with SSO privileges.

vto

**APPENDIX C**  
**SAMPLE LOGON PROCEDURE**

## APPENDIX C

### SAMPLE LOGON PROCEDURE

PROCEDURE MAINMENU LOGON FOR GENERAL USER POPULATION

\*\*\*\*\*

\* SAMPLE MAIN MENU PROGRAM \*

\*\*\*\*\*

```

DECLARE &PF                      INTEGER
DECLARE &INLIB                    STRING (8)
DECLARE &OUTLIB                   STRING (8)
DECLARE &RUNLIB                   STRING (8)
DECLARE &SPOOLIB                 STRING (8)
DECLARE &NAME                    STRING (24)

```

```

      EXTRACT  &NAME = USERNAME

```

```

DECLARE &ID                      STRING (3)

```

```

      EXTRACT  &ID = USERID

```

\*

```

ASSIGN  &INLIB    = &ID !! "WORK"
ASSIGN  &OUTLIB   = &ID !! "WORK"
ASSIGN  &RUNLIB   = &ID !! "WORK"
ASSIGN  &SPOOLIB = "#" !! &ID !! "PRT"

```

\*

```

SET PRNTMODE = H
SET INLIB=&INLIB, INVOL=VOLWORK
SET OUTLIB=&OUTLIB, OUTVOL=VOLWORK
SET RUNLIB=&RUNLIB, RUNVOL=VOLWORK
SET SPOOLIB=&SPOOLIB, SPOOLVOL=VOLWORK
SET WORKVOL=VOLWORK

```

\*

MENU:

```

PROMPT PFKEY = &PF
CENTER "**** HELLO," BRIGHT &NAME, " ****" ;;
CENTER "WELCOME TO THE USER MENU";;
CENTER "SELECT THE FUNCTION YOU WISH TO PERFORM";;
CENTER "PF 1   INVENTORY SYSTEM" ;;;
CENTER "PF 5   PROJECT LOG" ;;;
CENTER "PF 9   WORD PROCESSING" ;;;
CENTER "PF 16  LOGOFF THE SYSTEM" ;;

```

\*

```

IF &PF=1 GOTO INVENT
IF &PF=5 GOTO PRLOG
IF &PF=9 GOTO WPRUN
IF &PF=16 GOTO LOGOF
GOTO MENU

```

\*

```

INVENT:  RUN INVENTORY IN EXECLIB ON SYSVOL
GOTO MENU
PRLOG:   RUN PROJLOG IN PROJLIB ON SYSVOL
GOTO MENU
WPRUN:  RUN WP IN @SYSTEM@ ON SYSVOL
GOTO MENU
LOGOF:  LOGOFF

```

**APPENDIX D**  
**BIBLIOGRAPHY**

APPENDIX D  
BIBLIOGRAPHY

- A.I.D. Handbooks:   6 - Security  
                      18 - Information Services  
                      20 - Office Services  
                      23 - Overseas Support
- Department of Defense: Trusted Computer System Evaluation  
                          Criteria (August 15, 1983)
- Department of State: Information Systems Security Seminar  
                          for Security Officers
- Department of State: System Security Standard Number 3 -  
                          Security Standards for Unclassified Automated Information  
                          Systems at Foreign Service Posts (May 1985)
- Department of State: System Security Standard Number 4 -  
                          Security Standards for Unclassified Automated Information  
                          Systems in the United States
- Department of State: System Security Standard Number 5 -  
                          Security Standards for Unclassified Automated Information  
                          Systems Connectivity Worldwide (July 1987)
- Department of State Uniform Regulations: Security Regulations,  
                          Policy and Procedural Implementation of E.O. 12356  
                          (Handbook, dated December 23, 1983)
- WANG Laboratories publications:  
    Office Information Systems: Systems Administrator's Guide  
    WANG VS Procedure Language Reference Guide  
    WANG VS Systems Administrator's Learning Guide  
    WANG VS Systems Administrator's Reference Guide

**ATTACHMENT 1**

**A.I.D./W Notice from IG/SEC:**

**Processing LOU Material on WP and OIS Equipment in A.I.D./W  
(April 3, 1987)**

**AGENCY FOR INTERNATIONAL DEVELOPMENT**  
**WASHINGTON, D C 20523**

A.I.D./W Notice  
 IG/SEC  
 March 31, 1987  
 Issue Date: 4-3-87

**SUBJECT: Processing "Limited Official Use" (LOU) Material on Word Processor and Office Information Systems Equipment in A.I.D./Washington**

Para. 958.1, 5 FAM 900: "Certain sensitive official information and material which is not national security information and therefore, is not classifiable, nevertheless warrants a degree of protection. Such information or material may include, among other things, information received through privileged sources and certain personnel, medical, investigative, commercial, and financial records. Material of this type which requires limited dissemination shall be designated and marked Limited Official Use by any official having signing authority for the material. Such material shall be physically handled and transmitted as if it were "Confidential" and stored, at a minimum, in a barlock cabinet. The automated processing of LOU information must be accomplished in such a way as to minimize the potential for unauthorized access to this information. Responsible supervisors will assure that such automated processing is in compliance with established Departmental automation security guidelines."

Using the above guidelines, employees in A.I.D./Washington may process LOU material on word processing or office information systems equipment providing the following conditions are met:

- A. All LOU documents processed on word processing or office information systems equipment must be password protected. If the word processor or office information system does not have the capability of placing a password on LOU documents, it may NOT be used for processing LOU material.
- B. All tapes, magnetic cards, and floppy diskettes which are used for the storage of LOU material shall be secured (security container) at the close of each working day (para. 958.1, 5 FAM 900).

**However, remember: CONFIDENTIAL, SECRET, TOP SECRET WILL NOT BE PREPARED PROCESSED, OR STORED ON WORD PROCESSING AND OFFICE INFORMATION SYSTEMS EQUIPMENT.**

IG/SEC will make unscheduled visits throughout A.I.D./W to determine if classified material is being processed on office information systems. Security violations will be issued for documents prepared on non-TEMPEST approved equipment.

Questions should be referred to the Principal/Unit Security Officer, or to Mr. Robert G. Warren, IG/SEC, 235-9716.

**DISTRIBUTION:**  
**AID List H, Position 5**

**ATTACHMENT 2**

**Federal Information Resources Management Regulation  
(FIRMR) Bulletin 34:**

**Microcomputer Security  
(December 24, 1985)**

GENERAL SERVICES ADMINISTRATION  
Washington, DC 20405

December 24, 1985

FIRMR BULLETIN 34

TO: Heads of Federal agencies

SUBJECT: Microcomputer security

1. Purpose. This bulletin highlights the importance of agencies providing necessary security for their microcomputer systems. It is designed to reinforce the need for proper management of microcomputer systems and to provide general guidance on enhancing microcomputer security procedures.

2. Expiration date. This bulletin remains in effect until superseded or canceled.

3. Background.

a. The FIRMR provides that agencies shall establish an agency security program for their automated information systems, regardless of the equipment configuration of the systems (i.e., mainframes, minicomputers, or microcomputers). Many agencies have implemented security procedures for mainframes and minicomputers, but not for microcomputers (micros). Many magazine and newspaper articles have referenced the growing problem of micro abuse or misuse.

b. The "Counterfeit Access Device and Computer Fraud and Abuse Act of 1984" (Public Law 98-473 (18 U.S.C. 1030)) established misdemeanor and felony penalties for the abuse, unauthorized access, and misuse of Federally owned or operated computers including micros. Other legislative actions are currently undergoing congressional scrutiny.

4. Scope. This bulletin addresses only those general security measures that should be applied in order to establish and maintain a secure micro system. More specific security measures are explained by the National Bureau of Standards in NBS Special Publication 500-120, "Security of Personal Computer Systems: A Management Guide."

5. General.

a. Proper controls are critical for safeguarding micro systems against monetary loss and other adverse impacts on the agency's mission. OMB Circular No. A-130, dated December 12, 1985,

TC 84-8

## FIRMR Bulletin 34

establishes a minimum set of controls to be included in Federal automated information system security programs.

b. As with any other automated information system, the level of security for systems configured with micros is directly related to the degree of vulnerability and the value of the data stored. The level of protection afforded the micro configuration needs to be equivalent to the security level of any sensitive system that the micro accesses. In some cases, physical security of micros is not significantly different from the security of other non-ADP equipment used for office automation.

c. Security violations of micro systems often result from insufficient guidance concerning the importance of securing equipment, systems, and data processing information. It is essential that Federal agencies review current security measures that are applicable to micros. High-level officials need to clearly delegate responsibilities for achieving specific security goals for micros.

6. Security measures for micros. Some of the major goals of security management are: detection, correction, deterrence, prevention, and backup. The following methods are suggested for obtaining these goals.

a. Detection:

(1) A management official who is knowledgeable in data processing and security matters should be designated to monitor security for micro systems and report problems to the appropriate manager and/or higher-level official(s).

(2) Information on breaches in security of particular micro systems should be used as a warning to other users that similar breaches could occur on their system.

(3) Periodic review of security procedures should be used to detect possible defects in security.

(4) Micro users should be interviewed periodically for ideas to improve security, since some studies show that over half of the recent security breaches were detected and reported by users.

b. Correction:

(1) Immediate steps should be taken to correct any problems that have been detected or suspected.

(2) Internal policy and procedures should be revised as necessary to ensure that effective security measures are being implemented.

(3) Corrective efforts should be commensurate with the determined impact of monetary and mission loss.

c. Deterrence:

(1) Scramblers and encryption devices, approved by the National Security Agency, and keying material should be used, as appropriate, to deter easy access via telecommunication media.

(2) Security devices should be installed, as appropriate, to prevent theft of equipment.

(3) A lock over the "On and Off" switch should be used, as appropriate, to prevent easy access if the micro is in a non-secure location.

(4) Passwords of six or more characters, preferable a mixture of numbers and letters, should be used to make unauthorized access more difficult. Since passwords are often deciphered, overheard, or discovered by unauthorized persons, they should be changed periodically.

(5) The agency's microcomputer user group should periodically stress the importance of observing security procedures by offering seminars or meetings and providing messages or notes in newsletters on security issues.

(6) Both new and existing users of micro systems should be briefed periodically on Public Law 98-473 (18 U.S.C. 1030) and any other related laws.

d. Prevention:

(1) A risk analysis should be performed on micro system(s) used to process sensitive data, in determining threats, vulnerabilities, probability of occurrences, and loss impacts on the agency's mission.

## FIRMR Bulletin 34

(2) Micro users should observe the following common-sense guidance in securing their micros, floppy disks, peripherals, and user documentation.

(a) Do not post passwords on or near the micros, discuss them openly, or place them in any non-secure location, such as unlocked desks.

(b) Do not use the initials, birthdays or names of family, friends, or other easily decipherable names or initials for passwords.

(c) Do not leave micro accessories, copyrighted materials, or sensitive documents in an unlocked or easily accessible location.

(3) The designated management official should maintain an inventory listing or a security log that references the micro equipment and the person who is primarily responsible for that equipment.

e. Backup:

(1) Floppy disks that contain software or pertinent data should be duplicated, and the duplicate should be stored in a secure, compatible, and reasonably remote environment. However, copyright restrictions must not be violated.

(2) Identical micro systems should be located and used, as appropriate, as a backup facility if possible. (Note.--Compatibility with the backup system(s) must be tested and maintained to ensure its continued usefulness.)

7. Information and assistance.

a. Although most security guidance materials emphasize mainframes rather than micros, they can normally be adapted to micro security. A number of documents providing valuable guidance on security are listed in "Computer Security Publications," NBS Publications List 91. This list is available from:

Standards Processing Coordinator (ADP)  
 Institute for Computer Sciences and Technology  
 Technology Building, B-64  
 National Bureau of Standards  
 Gaithersburg, Maryland 20899  
 Telephone: (301) 921-3414 or FTS 921-3414

FIRMR Bulletin 34

b. Thorough training and maintaining knowledge of current trends in microcomputer security are keys to having secure systems. Many training programs and guidance materials are available to promote security for automated data processing equipment. Agency managers should seek training programs on micro security to ensure that their employees are and will be applying proper security measures.

c. Inquiries about the contents of this bulletin should be directed to Mary Anderson, Policy Branch (KMPP), telephone (202) 566-0194 or FTS, 566-0194.

  
FRANK J. CARR  
Commissioner  
Information Resources  
Management Service

ATTACHMENT 3

OMB Circular Number A-130:

Security of Federal Automated Information Systems  
(December 12, 1985)



EXECUTIVE OFFICE OF THE PRESIDENT  
OFFICE OF MANAGEMENT AND BUDGET  
WASHINGTON, D.C. 20503

December 12, 1985

CIRCULAR NO. A-130

TO THE HEADS OF EXECUTIVE DEPARTMENTS AND ESTABLISHMENTS

SUBJECT: Management of Federal Information Resources

1. Purpose: This Circular establishes policy for the management of Federal information resources. Procedural and analytic guidelines for implementing specific aspects of these policies are included as appendices.

2. Rescissions: This Circular rescinds OMB Circulars No. A-71, A-90, A-108, and A-121, and all Transmittal Memoranda to those circulars.

3. Authorities: This Circular is issued pursuant to the Paperwork Reduction Act of 1980 (44 U.S.C. 35); the Privacy Act of 1974 (5 U.S.C. 552a), Sections 111 and 206 of the Federal Property and Administrative Services Act of 1949 as amended (40 U.S.C. 759 and 487, respectively), the Budget and Accounting Act of 1921 as amended (31 U.S.C. 11), Executive Order No. 12046 of March 27, 1978, and Executive Order No. 12472 of April 3, 1984.

4. Applicability and Scope:

a. The policies in this Circular apply to the information activities of all agencies of the executive branch of the Federal Government.

b. Information classified for national security purposes should also be handled in accordance with the appropriate national security directives. National security emergency preparedness activities should be conducted in accordance with Executive Order No. 12472.

5. Background: The Paperwork Reduction Act establishes a broad mandate for agencies to perform their information management activities in an efficient, effective, and economical manner. To assist agencies in an integrated approach to information resources management, the Act requires that the Director of the Office of Management and Budget (OMB) develop and implement uniform and consistent information resources management policies; oversee the development and promote the use of information management principles, standards, and guidelines; evaluate agency information management practices in order to determine their adequacy and efficiency; and determine compliance of such practices with the policies, principles, standards, and guidelines promulgated by the Director.

60

6. Definitions: As used in this Circular--

a. The term "agency" means any executive department, military department, government corporation, government controlled corporation, or other establishment in the executive branch of the government, or any independent regulatory agency. Within the Executive Office of the President, the term includes only the Office of Management and Budget and the Office of Administration.

b. The term "information" means any communication or reception of knowledge such as facts, data, or opinions, including numerical, graphic, or narrative forms, whether oral or maintained in any medium, including computerized data bases, paper, microform, or magnetic tape.

c. The term "government information" means information created, collected, processed, transmitted, disseminated, used, stored, or disposed of by the Federal Government.

d. The term "information system" means the organized collection, processing, transmission, and dissemination of information in accordance with defined procedures, whether automated or manual.

e. The term "major information system" means an information system that requires special continuing management attention because of its importance to an agency mission; its high development, operating or maintenance costs; or its significant impact on the administration of agency programs, finances, property, or other resources.

f. The term "access to information" refers to the function of providing to members of the public, upon their request, the government information to which they are entitled under law.

g. The term "dissemination of information" refers to the function of distributing government information to the public, whether through printed documents, or electronic or other media. "Dissemination of information" does not include intra-agency use of information, interagency sharing of information, or responding to requests for "access to information."

h. The term "information technology" means the hardware and software used in connection with government information, regardless of the technology involved, whether computers, telecommunications, micrographics, or others. For the purposes of this Circular, automatic data processing and telecommunications activities related to certain critical national security missions, as defined in 44 U.S.C. 3502 (2) and 50 U.S.C. 2315, are excluded.

61

i. The term "information technology facility" means an organizationally defined set of personnel, hardware, software, and physical facilities, a primary function of which is the operation of information technology.

j. The term "information resources management" means the planning, budgeting, organizing, directing, training, and control associated with government information. The term encompasses both information itself and the related resources, such as personnel, equipment, funds, and technology.

k. The term "government publication" means informational matter which is published as an individual document at government expense, or as required by law.

Other definitions specific to the subjects of the appendices appear in the appendices.

## 7. Basic Considerations and Assumptions

a. The Federal Government is the largest single producer, consumer, and disseminator of information in the United States. Because of the size of the government's information activities, the dependence of government information activities upon the public's cooperation, and the value of government information to the entire Nation, the management of Federal information resources is an issue of continuing importance to the public and to the government itself.

b. Government information is a valuable national resource. It provides citizens with knowledge of their government, society, and economy--past, present, and future; is a means to ensure the accountability of government; is vital to the healthy performance of the economy; is an essential tool for managing the government's operations; and is itself a commodity often with economic value in the marketplace.

c. The free flow of information from the government to its citizens and vice versa is essential to a democratic society. It is also essential that the government minimize the Federal paperwork burden on the public, minimize the cost of its information activities, and maximize the usefulness of government information.

d. In order to minimize the cost and maximize the usefulness of government information activities, the expected public and private benefits derived from government information, insofar as they are calculable, should exceed the public and private costs of the information.

e. Although certain functions are inherently governmental in nature, being so intimately related to the public interest as to mandate performance by Federal employees, the government

should look first to private sources, where available, to provide the commercial goods and services needed by the government to act on the public's behalf, particularly when cost comparisons indicate that private performance will be the most economical.

f. The use of up-to-date information technology offers opportunities to improve the management of government programs, and access to, and dissemination of, government information.

g. Because the public disclosure of government information is essential to the operation of a democracy, the public's right of access to government information must be protected in the management of Federal information resources.

h. The individual's right to privacy must be protected in Federal Government information activities involving personal information.

i. The open and efficient exchange of government scientific and technical information, subject to applicable national security controls and proprietary rights others may have in such information, fosters excellence in scientific research and the effective use of Federal research and development funds.

j. The value of preserving government records is a function of the degree to which preservation protects the legal and financial rights of the government or its citizens, and provides an official record of Federal agency activities for agency management, public accountability, and historical purposes.

k. Federal Government information resources management policies and activities can affect, and be affected by, the information policies and activities of other nations.

## 8. Policies

### a. Information Management. Agencies shall:

(1) Create or collect only that information necessary for the proper performance of agency functions and that has practical utility, and only after planning for its processing, transmission, dissemination, use, storage, and disposition;

(2) Seek to satisfy new information needs through legally authorized interagency or intergovernmental sharing of information, or through commercial sources, where appropriate, before creating or collecting new information;

(3) Limit the collection of individually identifiable information and proprietary information to that which is legally authorized and necessary for the proper performance of agency functions;

(4) Maintain and protect individually identifiable information and proprietary information in a manner that precludes:

(a) Unwarranted intrusion upon personal privacy (see Appendix I); and

(b) Violation of confidentiality;

(5) Provide individuals with access to, and the ability to amend errors in, systems of records, consistent with the Privacy Act;

(6) Provide public access to government information, consistent with the Freedom of Information Act;

(7) Ensure that agency personnel are trained to safeguard information resources;

(8) Disseminate information, as required by law, describing agency organization, activities, programs, meetings, systems of records, and other information holdings, and how the public may gain access to agency information resources;

(9) Disseminate such information products and services as are:

(a) Specifically required by law; or

(b) Necessary for the proper performance of agency functions, provided that the latter do not duplicate similar products or services that are or would otherwise be provided by other government or private sector organizations;

(10) Disseminate significant new, or terminate significant existing, information products and services only after providing adequate notice to the public;

(11) Disseminate such government information products and services:

(a) In a manner that ensures that members of the public whom the agency has an obligation to reach have a reasonable ability to acquire the information;

(b) In the manner most cost effective for the government, including placing maximum feasible reliance on the private sector for the dissemination of the products or services in accordance with OMB Circular No. A-76; and

(c) So as to recover costs of disseminating the products or services through user charges, where appropriate, in accordance with OMB Circular No. A-25;

b4

## (12) Establish procedures for:

(a) Reviewing periodically the continued need for and manner of dissemination of the agency's information products or services; and

(b) Ensuring that government publications are made available to depository libraries as required by law.

b. Information Systems and Information Technology Management. Agencies shall:

(1) Establish multiyear strategic planning processes for acquiring and operating information technology that meet program and mission needs, reflect budget constraints, and form the bases for their budget requests;

(2) Establish systems of management control that document the requirements that each major information system is intended to serve; and provide for periodic review of those requirements over the life of the system in order to determine whether the requirements continue to exist and the system continues to meet the purposes for which it was developed;

(3) Make the official whose program an information system supports responsible and accountable for the products of that system;

(4) Meet information processing needs through interagency sharing and from commercial sources, when it is cost effective, before acquiring new information processing capacity;

(5) Share available information processing capacity with other agencies to the extent practicable and legally permissible;

(6) Acquire information technology in a competitive manner that minimizes total life cycle costs;

(7) Ensure that existing and planned major information systems do not unnecessarily duplicate information systems available from other agencies or from the private sector;

(8) Acquire off-the-shelf software from commercial sources, unless the cost effectiveness of developing custom software is clear and has been documented;

(9) Acquire or develop information systems in a manner that facilitates necessary compatibility;

(10) Assure that information systems operate effectively and accurately;

65

(11) Establish a level of security for all agency information systems commensurate with the sensitivity of the information and the risk and magnitude of loss or harm that could result from improper operation of the information systems (See Appendix III);

(12) Assure that only authorized personnel have access to information systems;

(13) Plan to provide information systems with reasonable continuity of support should their normal operations be disrupted in an emergency;

(14) Use Federal Information Processing and Telecommunications Standards except where it can be demonstrated that the costs of using a standard exceed the benefits or the standard will impede the agency in accomplishing its mission;

(15) Not require program managers to use specific information technology facilities or services unless it is clear and is convincingly documented, subject to periodic review, that such use is the most cost effective method for meeting program requirements;

(16) Account for the full costs of operating information technology facilities and recover such costs from government users as provided in Appendix II;

(17) Not prescribe Federal information system requirements that unduly restrict the prerogatives of heads of State and local government units;

(18) Seek opportunities to improve the operation of government programs or to realize savings for the government and the public through the application of up-to-date information technology to government information activities.

## 9. Assignment of Responsibilities:

### a. All Federal Agencies. The head of each agency shall:

(1) Have primary responsibility for managing agency information resources;

(2) Ensure that the information policies, principles, standards, guidelines, rules, and regulations prescribed by OMB are implemented appropriately within the agency;

(3) Develop internal agency information policies and procedures and oversee, evaluate, and otherwise periodically review agency information resources management activities for conformity with the policies set forth in this Circular;

(4) Develop agency policies and procedures that provide for timely acquisition of required information technology;

(5) Maintain an inventory of the agencies' major information systems and information dissemination programs;

(6) Create, maintain, and dispose of a record of agency activities in accordance with the Federal Records Act of 1950, as amended;

(7) Identify to the Director, OMB, statutory, regulatory, and other impediments to efficient management of Federal information resources and recommend to the Director legislation, policies, procedures, and other guidance to improve such management;

(8) Assist OMB in the performance of its functions under the Paperwork Reduction Act, including making services, personnel, and facilities available to OMB for this purpose to the extent practicable;

(9) Appoint a senior official, as required by 44 U.S.C. 3506(b), who shall report directly to the agency head, to carry out the responsibilities of the agency under the Paperwork Reduction Act. The head of the agency shall keep the Director, OMB, advised as to the name, title, authority, responsibilities, and organizational resources of the senior official. For purposes of this paragraph military departments and the Office of the Secretary of Defense may each appoint one official.

b. Department of State. The Secretary of State shall:

(1) Advise the Director, OMB, on the development of United States positions and policies on international information policy issues affecting Federal Government information activities and ensure that such positions and policies are consistent with Federal information resources management policy;

(2) Ensure, in consultation with the Secretary of Commerce, that the United States is represented in the development of international information technology standards, and advise the Director, OMB, of such activities.

c. Department of Commerce. The Secretary of Commerce shall:

(1) Develop and issue Federal Information Processing Standards and guidelines necessary to ensure the efficient and effective acquisition, management, security, and use of information technology;

(2) Advise the Director, OMB, on the development of policies relating to the procurement and management of Federal telecommunications resources;

(3) Provide OMB and the agencies with scientific and technical advisory services relating to the development and use of information technology;

(4) Conduct studies and evaluations concerning telecommunications technology, and concerning the improvement, expansion, testing, operation, and use of Federal telecommunications systems and advise the Director, OMB, and appropriate agencies of the recommendations that result from such studies;

(5) Develop, in consultation with the Secretary of State and the Director, OMB, plans, policies, and programs relating to international telecommunications issues affecting government information activities;

(6) Identify needs for standardization of telecommunications and information processing technology, and develop standards, in consultation with the Secretary of Defense and the Administrator of General Services, to ensure efficient application of such technology;

(7) Ensure that the Federal Government is represented in the development of national and, in consultation with the Secretary of State, international information technology standards, and advise the Director, OMB, of such activities.

d. Department of Defense. The Secretary of Defense shall develop, in consultation with the Administrator of General Services, uniform Federal telecommunications standards and guidelines to ensure national security, emergency preparedness, and continuity of government.

e. General Services Administration. The Administrator of General Services shall:

(1) Advise the Director, OMB, and agency heads on matters affecting the procurement of information technology;

(2) Coordinate and, when required, provide for the purchase, lease, and maintenance of information technology required by Federal agencies;

(3) Develop criteria for timely procurement of information technology and delegate procurement authority to agencies that comply with the criteria;

(4) Provide guidelines and regulations for Federal agencies, as authorized by law, on the acquisition, maintenance, and disposition of information technology;

(5) Develop policies and guidelines that facilitate the sharing of information technology among agencies as required by this Circular;

(6) Review agencies' information resources management activities to meet the objectives of the triennial reviews required by the Paperwork Reduction Act and report the results to the Director, OMB;

(7) Manage the Automatic Data Processing Fund and the Federal Telecommunications Fund in accordance with the Federal Property and Administrative Services Act, as amended;

(8) Establish procedures for approval, implementation, and dissemination of Federal telecommunications standards and guidelines and for implementation of Federal Information Processing Standards.

f. Office of Personnel Management. The Director, Office of Personnel Management, shall:

(1) Develop and conduct training programs for Federal personnel on information resources management, including end user computing;

(2) Evaluate periodically future personnel management and staffing requirements for Federal information resources management;

(3) Establish personnel security policies and develop training programs for Federal personnel associated with the design, operation, or maintenance of information systems.

g. National Archives and Records Administration. The Archivist of the United States shall:

(1) Administer the Federal records management program in accordance with the National Archives and Records Act;

(2) Assist the Director, OMB, in developing standards and guidelines relating to the records management program.

h. Office of Management and Budget. The Director of the Office of Management and Budget shall:

(1) Provide overall leadership and coordination of Federal information resources management within the executive branch;

(2) Serve as the President's principal adviser on procurement and management of Federal telecommunications systems, and develop and establish policies for procurement and management of such systems;

(3) Issue policies, procedures, and guidelines to assist agencies in achieving integrated, effective, and efficient information resources management;

(4) Initiate and review proposals for changes in legislation, regulations, and agency procedures to improve Federal information resources management;

(5) Review and approve or disapprove agency proposals for collection of information from the public, as defined in 5 CFR 1320.7;

(6) Develop and publish annually, in consultation with the Administrator of General Services, a five-year plan for meeting the information technology needs of the Federal government;

(7) Evaluate agencies' information resources management and identify cross-cutting information policy issues through the review of agency information programs, information collection budgets, information technology acquisition plans, fiscal budgets, and by other means;

(8) Provide policy oversight for the Federal records management function conducted by the National Archives and Records Administration and coordinate records management policies and programs with other information activities;

(9) Review, with the advice and assistance of the Administrator of General Services, selected agencies' information resources management activities to meet the objectives of the triennial reviews required by the Paperwork Reduction Act;

(10) Review agencies' policies, practices, and programs pertaining to the security, protection, sharing, and disclosure of information, in order to ensure compliance with the Privacy Act and related statutes;

(11) Resolve information technology procurement disputes between agencies and the General Services Administration pursuant to Section 111 of the Federal Property and Administrative Services Act;

(12) Review proposed U.S. government position and policy statements on international issues affecting Federal Government information activities and advise the Secretary of State as to their consistency with Federal information resources management policy.

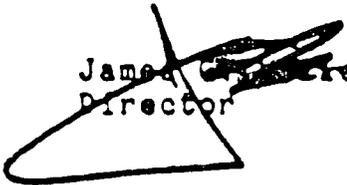
10. Oversight. The Director, OMB, will use information technology planning reviews, fiscal budget reviews, information collection budget reviews, management reviews, GSA reviews of agency information resources management activities, and such

other measures as he deems necessary to evaluate the adequacy and efficiency of each agency's information resources management and compliance with this Circular.

11. Effective Date. This Circular is effective upon publication.

12. Inquiries. All questions or inquiries should be addressed to Office of Information and Regulatory Affairs, Office of Management and Budget, Washington, D.C. 20503. Telephone: (202) 395-3287.

13. Sunset Review Date. This Circular shall have an independent policy review to ascertain its effectiveness three years from the date of issuance.

  
James C. Crer III  
Director

Appendix I: Federal Agency Responsibilities for Maintaining Records about Individuals

Appendix II: Cost Accounting, Cost Recovery, and Interagency Sharing of Information Technology Facilities

Appendix III: Security of Federal Automated Information Systems

Appendix IV: Analysis of Key Sections

APPENDIX I  
TO OMB CIRCULAR NO. A-130  
:  
FEDERAL AGENCY RESPONSIBILITIES FOR MAINTAINING  
RECORDS ABOUT INDIVIDUALS

1. Purpose and Scope

This Appendix describes agency responsibilities for implementing the Privacy Act of 1974, 5 U.S.C. 552a as amended (hereinafter "the Act"). It applies to all agencies subject to the Act. The Appendix constitutes a revision to procedures formerly contained in OMB Circular No. A-108, now rescinded. Note that this Appendix does not rescind other guidance OMB has issued to help agencies interpret the Privacy Act's provisions, e.g., Privacy Act Guidelines (40 Federal Register 28949-28978, July 9, 1975), or Guidance for Conducting Matching Programs (47 Federal Register 21656-21658, May 19, 1982).

2. Definitions

a. The terms "agency," "individual," "maintain," "record," "system of records," and "routine use," as used in this Appendix, are defined in the Act (5 U.S.C. 552a (a)). The definition of "agency" in the Act differs somewhat from the definition in the Circular.

b. The term "minor change to a system of records" means a change that does not significantly change the system; that is, does not affect the character or purpose of the system and does not affect the ability of an individual to gain access to his or her record or to any information pertaining to him or her which is contained in the system; e.g., changing the title of the system manager.

3. Assignment of Responsibilities

a. All Federal Agencies. In addition to meeting the agency requirements contained in the Act, and the specific reporting requirements detailed in this Appendix, the head of each agency shall ensure that the following reviews are conducted as often as specified below, and be prepared to report to the Director, OMB, the results of such reviews and the corrective action taken to resolve problems uncovered. The head of each agency shall:

(1) Section (m) Contracts. Review every two years a random sample of agency contracts that provide for the maintenance of a system of records on behalf of the agency to

accomplish an agency function, in order to ensure that the wording of each contract makes the provisions of the Act apply. (5 U.S.C. 552a (m)(1))

(2) Recordkeeping Practices. Review annually agency recordkeeping and disposal policies and practices in order to assure compliance with the Act.

(3) Routine Use Disclosures. Review every three years the routine use disclosures associated with each system of records in order to ensure that the recipient's use of such records continues to be compatible with the purpose for which the disclosing agency originally collected the information. The first such review should commence immediately upon the issuance of this Appendix.

(4) Exemption of Systems of Records. Review every three years each system of records for which the agency has promulgated exemption rules pursuant to Section (j) or (k) of the Privacy Act in order to determine whether such exemption is still needed.

(5) Matching Programs. Review annually each ongoing matching program in which the agency has participated during the year, either as a source or as a matching agency, in order to ensure that the requirements of the Act, the OMB Matching Guidelines, and the OMB Model Control System and Checklist have been met.

(6) Privacy Act Training. Review annually agency training practices in order to ensure that all agency personnel are familiar with the requirements of the Act, with the agency's implementing regulation, and with any special requirements that their specific jobs entail.

(7) Violations. Review annually the actions of agency personnel that have resulted either in the agency being found civilly liable under Section (g) of the Act, or an employee being found criminally liable under the provisions of Section (i) of the Act, in order to determine the extent of the problem and to find the most effective way to prevent recurrences of the problem.

(8) Systems of Records Notices. Review annually each system of records notice to ensure that it accurately describes the system. Where minor changes are needed, ensure that an amended notice is published in the Federal Register. Agencies may choose to make one annual comprehensive publication consolidating such minor changes. This requirement is distinguished from and in addition to the requirement to report to OMB and the Congress major changes to systems of records and to publish those changes in the Federal Register (see paragraph 4b of this Appendix).

b. Department of Commerce. The Secretary of Commerce shall, consistent with guidelines issued by the Director, OMB, develop and issue standards and guidelines for assuring the security of information protected by the Privacy Act in automated information systems.

c. General Services Administration. The Administrator of General Services shall, consistent with guidelines issued by the Director, OMB, issue instructions on what agencies must do in order to comply with the requirements of Section (m) of the Act when contracting for the operation of a system of records to accomplish an agency purpose.

d. Office of Personnel Management. The Director of the Office of Personnel Management shall, consistent with guidelines issued by the Director, OMB:

(1) Develop and maintain government-wide standards and procedures for civilian personnel information processing and recordkeeping directives to assure conformance with the Act.

(2) Develop and conduct training programs for agency personnel, including both the conduct of courses in various substantive areas (e.g., legal, administrative, information technology) and the development of materials that agencies can use in their own courses. The assignment of this responsibility to OPM does not affect the responsibility of individual agency heads for developing and conducting training programs tailored to the specific needs of their own personnel.

e. National Archives and Records Administration. The Archivist of the United States shall, consistent with guidelines issued by the Director, OMB:

(1) Issue instructions on the format of the agency notices and rules required to be published under the Act.

(2) Compile and publish annually the rules promulgated under 5 U.S.C. 552a(f) and agency notices published under 5 U.S.C. 552a (e)(4) in a form available to the public.

(3) Issue procedures governing the transfer of records to Federal Records Centers for storage, processing, and servicing pursuant to 44 U.S.C. 3103. For purposes of the Act, such records are considered to be maintained by the agency that deposited them. The Archivist may disclose deposited records only according to the access rules established by the agency that deposited them.

f. Office of Management and Budget. The Director of the Office of Management and Budget will:

(1) Issue guidelines and directives to the agencies to implement the Act.

(2) Assist the agencies, at their request, in implementing their Privacy Act programs.

(3) Review the new and altered system reports agencies submit pursuant to Section (o) of the Act.

(4) Compile the annual report of the President to the Congress in accordance with Section (p) of the Act.

#### 4. Reporting Requirements

a. Privacy Act Annual Reports. To provide the necessary information for the annual report of the President, agencies shall submit a Privacy Act Annual Report to the Director, OMB, covering their Privacy Act activities for the calendar year. The exact format and timing of the report will be established by the Director, OMB. (5 U.S.C. 552a (p)); but, agencies should, at a minimum collect, and be prepared to report the following data on a calendar year basis:

(1) Total number of active systems of records and changes to that population during the year, e.g., publications of new systems, additions and deletions of routine uses, exemptions, automation of record systems.

(2) Public comments received on agency publications and implementation activities.

(3) Number of requests from individuals for access to records about themselves in systems of records that cited the Privacy Act in support of their requests.

(4) Number granted in whole or part, denied in whole, and for which no record was found.

(5) Number of amendment requests from individuals to amend records about them in systems of records that cited the Privacy Act in support of their requests.

(6) Number granted in whole or part, denied in whole, and for which no record was found.

(7) Number of appeals of access and amendment denials and the results of such appeals.

(8) Number of instances in which individuals litigated the results of appeals of access or amendment, and the results of such litigation.

(9) Number and description of matching programs participated in either as source or matching agency.

b. New and Altered System Reports. The Act requires agencies to publish notices in the Federal Register describing new or altered systems of records, and to submit reports on these systems to the Director, OMB, and to the Congress.

(1) Altered System of Records. Minor changes to systems of records need not be reported. For example, a change in the designation of the system manager due to a reorganization would not require a report, so long as an individual's ability to gain access to his or her records is not affected. Other examples include changing applicable safeguards as a result of a risk analysis, deleting a routine use when there is no longer a need for the authorized disclosure. These examples are not intended to be all-inclusive.

The following changes are those for which a report is required:

(a) An increase or change in the number or types of individuals on whom records are maintained. For example, a decision to expand a system that originally covered only residents of public housing in major cities to cover such residents nationwide would require a report. Increases attributable to normal growth should not be reported.

(b) A change that expands the types or categories of information maintained. For example, a personnel file that has been expanded to include medical records would require a report.

(c) A change that alters the purpose for which the information is used.

(d) A change to equipment configuration (either hardware or software) that creates substantially greater access to the records in the system. For example, locating interactive terminals at regional offices for accessing a system formerly accessible only at the headquarters would require a report.

(e) The addition of an exemption (pursuant to Sections (j) or (k) of the Act). Note that, in submitting a rulemaking for an exemption as part of a report of a new or altered system, agencies will meet the reporting requirements of Executive Order No. 12291 and need not make a separate submission under that order.

When an agency makes a change to an information technology installation, telecommunication network, or any other general changes in information collection, processing, dissemination, or storage that affect multiple systems of records, it may submit a single consolidated new or altered system report, with changes to existing notices and supporting documentation included in the submission.

(2) Contents of the Report. The report for a new or altered system has three elements: a transmittal letter, a narrative statement, and supporting documentation that includes a copy of the proposed Federal Register notice. There is no prescribed format for either the letter or the narrative statement. The notice must appear in the format prescribed by the Office of the Federal Register's Document Drafting Handbook.

(a) Transmittal Letter. The transmittal letter should be signed by the senior agency official responsible for implementation of the Act within the agency and should contain the name and telephone number of the individual who can best answer questions about the system. The letter should contain the agency's assurance that the proposed system does not duplicate any existing agency systems. It should also state that a copy of the report has been distributed to the Speaker of the House and the President of the Senate as the Act requires. The letter may also include requests for waiver of the reporting time period.

(b) Narrative Statement. The narrative statement should be brief. It should make reference, as appropriate, to information in the supporting documentation rather than restating such information. The statement should:

1 Describe the purpose for which the agency is establishing the system of records.

2 Identify the authority under which the system is maintained. The agency should avoid citing housekeeping statutes, but rather cite the underlying programmatic authority for collecting, maintaining, and using the information. When the system is being operated to support an agency housekeeping program, e.g., a carpool locator, the agency may, however, cite a general housekeeping statute that authorizes the agency head to keep such records as are necessary.

3 Provide the agency's evaluation of the probable or potential effects of the proposal on the privacy of individuals.

4 Describe the relationship of the proposal, if any, to the other branches of the Federal Government and to State and local governments.

5 Provide a brief description of the steps taken by the agency to minimize the risk of unauthorized access to the system of records. A more detailed assessment of the risks and specific administrative, technical, procedural, and physical safeguards established shall be made available to OMB upon request.

6 Explain how each proposed routine use satisfies the compatibility requirement of subsection (a)(7) of the Act. For altered systems, this requirement pertains only to any newly proposed routine uses.

7 Provide OMB control numbers, expiration dates, and titles of any OMB approved information collection requirements contained in the system of records. If the request for OMB clearance of an information collection is pending, the agency may simply state the title of the collection and the date it was submitted for OMB clearance.

(c) Supporting Documentation. Attach the following to all new or altered system reports:

1 An advance copy of the new or altered system notice (consistent with the provisions of 5 U.S.C. 552a (e)(4)) that the agency proposes to publish for the new or altered system. For proposed altered systems the documentation should be in the same form as the agency proposes to publish in the public notice.

2 An advance copy of any new rules or changes to published rules (consistent with the provision of 5 U.S.C. 552a (f), (j), and (k)) that the agency proposes to issue for the new or altered system. If no changes to existing rules are required, the agency shall so state in the narrative portion of the report. Proposed changes to existing rules shall be provided in the same form as the agency proposes to publish for formal notice and comment.

(3) Timing and Distribution for Submitting New and Altered System Reports. Submit reports on new and altered systems of records not later than 60 days prior to establishment of a new system or the implementation of an altered system (5 U.S.C. 552a (o)). Submit three copies of each report to:

President of the Senate  
Washington, D.C. 20510

Speaker of the House of Representatives  
Washington, D.C. 20515

Administrator  
Office of Information and Regulatory Affairs  
Office of Management and Budget  
Washington, D.C. 20503

Agencies may assume that OMB concurs in Privacy Act aspects of their proposal if OMB has not commented within 60 days from the date the transmittal letter was signed. Agencies may publish system and routine use notices as well as exemption rules in the Federal Register at the same time that they send the new or

altered system report to OMB and the Congress. The 60 day period for OMB and Congressional review and the 30 day notice and comment period for routine uses and exemptions will then run concurrently.

(4) Waivers of Report Time Period. The Director, OMB, may grant a waiver of the 60 day period if the agency asks for the waiver and can demonstrate compelling reasons. Agencies may assume that OMB concurs in their request if OMB has not commented within 30 days of the date the transmittal letter was signed. When a waiver is granted, the agency is not thereby relieved of any other responsibility or liability under the Act. Note that OMB cannot waive time periods specifically established by the Act. Agencies will still have to meet the statutory notice and comment periods required for establishing a routine use or claiming an exemption.

APPENDIX II  
TO OMB CIRCULAR NO. A-130

COST ACCOUNTING, COST RECOVERY, AND INTERAGENCY  
SHARING OF INFORMATION TECHNOLOGY FACILITIES

1. Purpose

This Appendix establishes procedures for cost accounting, cost recovery, and interagency sharing of Federal information technology facilities. The Appendix revises procedures formerly contained in OMB Circular No. A-121, now rescinded.

2. Applicability

This Appendix applies to all information technology facilities that are operated by or on behalf of a Federal agency; provide information technology service to more than one user; operate one or more general management computers; and have obligations in excess of \$3 million per year.

3. Definitions

a. The term "information technology facility" means an organizationally defined set of personnel, hardware, software, and physical facilities, a primary function of which is the operation of information technology. An information technology facility includes:

(1) The personnel who operate computers or telecommunications systems; develop or maintain software; provide user liaison and training; schedule computers, prepare and control input data; control, reproduce, and distribute output data; maintain tape and disk libraries; provide security, maintenance, and custodial services; and directly manage or provide direct administrative support to personnel engaged in these activities.

(2) The owned or leased computer and telecommunications hardware, including central processing units; associated peripheral equipment such as disk drives, tape drives, drum storage, printers, card readers, and consoles; data entry equipment; data reproduction, decollation, booking, and binding equipment; telecommunications equipment including control units, terminals, modems, and dedicated telephone and satellite links provided by the facility to enable data transfer and access to users. Hardware acquired and maintained by users of the facility is excluded.

(3) The software, including operating system software, utilities, sorts, language processors, access methods, data base processors, and other similar multi-user software required by the

facility for support of the facility and/or for general use by users of the facility. All software acquired or maintained by users of the facility is excluded.

(4) The physical facilities, including computer rooms; tape and disk libraries; stockrooms and warehouse space; office space; physical fixtures.

b. The term "full costs" means all significant expenses incurred in the operation of an information technology facility. The following elements are included:

(1) Personnel, including salaries, overtime, and fringe benefits of civilian and military personnel; training; and travel.

(2) Equipment, including depreciation for owned, capitalized equipment; equipment rental or lease; and direct expenses for noncapitalized equipment.

(3) Software, including depreciation for capitalized costs of developing, converting, or acquiring software; rental of for software; and direct expenses for noncapitalized acquisition of software.

(4) Supplies, including office supplies; data processing materials; and miscellaneous expenses.

(5) Contracted services, including technical and consulting services; equipment maintenance; data entry support; operations support; facilities management; maintenance of software; and telecommunications network services.

(6) Space occupancy, including rental and lease of buildings, general office furniture, and equipment; building maintenance; heating, air conditioning and other utilities; telephone services; power conditioning and distribution equipment and alternate power sources; and building security and custodial services.

(7) Intra-agency services, including normal agency support services that are paid by the installation.

(8) Interagency services, including services provided by other agencies and departments that are paid by the installation.

c. The term "user" means an organizational or programmatic entity that receives service from an information technology facility. A user may be either internal or external to the agency organization responsible for the facility, but normally does not report either to the manager or director of the facility or to the same immediate supervisor.

d. The term "general management computer" means a digital computer that is used for any purpose other than as a part of a process control system, space system, mobile system, or a system meeting one of the exclusions identified in the Department of Defense Authorization Act of 1982.

#### 4. Accounting and Reimbursement for Sharing of Information Technology Facilities

##### a. Interagency Sharing. Agencies shall:

(1) Share their information technology facilities with users from other agencies to the maximum extent feasible;

(2) Document sharing arrangements, where the total annual reimbursement exceeds \$500,000, with individual written agreements that identify:

(a) Services available for sharing;

(b) Service priority procedures and terms (e.g., quality performance standards) to be provided to each user;

(c) Prices to be charged for providing services;

(d) Reimbursement arrangements for services provided; and

(e) Arrangements for terminating the sharing agreement;

(3) Provide standard terms and conditions to users obtaining similar services insofar as possible;

(4) Include such sharing arrangements, when fully documented and part of a formal sharing program, in justifications to OMB for resource requests (see OMB Circular No. A-11, revised) and allocations. Direct funding by a shared facility should be requested only where exceptional circumstances preclude the user agency from using alternative sources.

b. Cost Accounting. Agencies shall account for the full cost of the operation of information technology facilities.

c. User Cost Distribution System. Agencies shall implement a system to distribute the full cost of providing services to all users. That system will:

(1) Be consistent with guidance provided in the Federal Information Processing Standards Publication No. 96, "Guidelines for Developing and Implementing a Charging System for Data Processing Services" (National Bureau of Standards, Department of Commerce, 1982).

(2) Price each service provided by the facility to the users of that service on an equitable basis commensurate with the amount of resources required to provide that service and the priority of service provided. The price of individual transactions may be estimated provided that they are periodically reconciled to assure that the full costs of operations are equitably distributed among all users.

(3) Directly distribute to the recipient of the services the full costs of dedicated services, including applications developed and maintained; software unique to a single application; and telecommunications equipment, including control units, terminals, modems, and dedicated telephone or satellite links provided by the facility to enable data transfer and computer access to users.

d. Cost Recovery. Consistent with statutory authority, agencies shall:

(1) Submit periodic statements to all users of agency information technology facilities specifying the costs of services provided;

(2) Recover full costs from Federal users of the facility; and

(3) Recover costs from nonfederal users of the facilities consistent with OMB Circular No. A-25.

e. Accounting for Reimbursements Received. Agencies shall:

(1) Include resource requests for the amount of planned information technology use in user budget and appropriation requests;

(2) Assure that shared facilities reduce budget and appropriation requests by the amount of planned reimbursements from users;

(3) Prepare, at the close of each fiscal year, a report that documents in the agency's official records the full past year cost of operating information technology facilities that recover more than \$500,000 per year from sharing reimbursements; and

(4) Use the portion of reimbursements arising from equipment and software depreciation for the replacement of equipment and software capital assets, provided such usage is included in the agency's budget.

## 5. Selection of Information Technology Facilities to Support New Applications.

In selecting information technology facilities to support new applications, agencies shall establish a management control procedure for determining which facility will be used to support each significant application. This procedure shall ensure that:

- (a) All alternative facilities are considered, including other Federal agency and nonfederal facilities and services;
- (b) Agency rules do not require that priority be given to the use of in-house facilities; and
- (c) The user of the application has primary responsibility for selecting the facility.

## 6. Assignment of Responsibilities

a. All Federal Agencies. The head of each agency shall:

- (1) Establish policies and procedures and assign responsibilities to implement the requirements of this Appendix; and
- (2) Ensure that contracts awarded for the operation of information technology facilities include provisions for compliance with the requirements of this Appendix.

b. General Services Administration. The Administrator of General Services shall:

- (1) Ensure that information technology facilities designated as Federal Data Processing Centers comply with the procedures established by this Appendix;
- (2) Ensure that provisions consistent with this Appendix are included in contracts for the operation of information technology facilities when acquiring services on behalf of an agency;

## 7. Implementation Requirements

Agencies shall implement the provisions of this Appendix effective at the beginning of fiscal year 1987.

APPENDIX III  
TO OMB CIRCULAR NO. A-130

SECURITY OF FEDERAL AUTOMATED INFORMATION SYSTEMS

1. Purpose

This Appendix establishes a minimum set of controls to be included in Federal automated information systems security programs; assigns responsibilities for the security of agency automated information systems; and clarifies the relationship between such agency security programs and internal control systems established in accordance with OMB Circular No. A-123, Internal Control Systems. The Appendix revises procedures formerly contained in Transmittal Memorandum No. 1 to OMB Circular No. A-71, now rescinded, and incorporates responsibilities from applicable national security directives.

2. Definitions

a. The term "automated information system" means an information system (defined in Section 6d of the Circular) that is automated.

b. The term "information technology installation" means one or more computer or office automation systems including related telecommunications, peripheral and storage units, central processing units, and operating and support system software. Information technology installations may range from information technology facilities such as large centralized computer centers to individual stand-alone microprocessors such as personal computers.

c. The term "sensitive data" means data that require protection due to the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the data. The term includes data whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary data, records about individuals requiring protection under the Privacy Act, and data not releasable under the Freedom of Information Act

d. The term "sensitive application" means an application of information technology that requires protection because it processes sensitive data, or because of the risk and magnitude of loss or harm that could result from improper operation or deliberate manipulation of the application.

e. The term "security specifications" means a detailed description of the safeguards required to protect a sensitive application.

### 3. Automated Information Systems Security Programs

Agencies shall assure an adequate level of security for all agency automated information systems, whether maintained in-house or commercially. Specifically, agencies shall:

- Assure that automated information systems operate effectively and accurately;
- Assure that there are appropriate technical, personnel, administrative, environmental, and telecommunications safeguards in automated information systems; and
- Assure the continuity of operation of automated information systems that support critical agency functions.

Agencies shall implement and maintain an automated information systems security program, including the preparation of policies, standards, and procedures. This program will be consistent with government-wide policies, procedures, and standards issued by the Office of Management and Budget, the Department of Commerce, the Department of Defense, the General Services Administration, and the Office of Personnel Management. Agency programs shall incorporate additional requirements for securing national security information in accordance with appropriate national security directives. Agency programs shall, at a minimum, include four primary elements: applications security, personnel security, information technology installation security, and security awareness and training.

#### a. Applications Security

(1) Management Control Process and Sensitivity Evaluation. Agencies shall establish a management control process to assure that appropriate administrative, physical, and technical safeguards are incorporated into all new applications, and into significant modifications to existing applications. Management officials who are the primary users of applications should evaluate the sensitivity of new or existing applications being substantially modified. For those applications considered sensitive, the management control process shall, at a minimum, include security specifications and design reviews and systems tests.

(a) Security Specifications. Agencies shall define and approve security requirements and specifications prior to acquiring or starting formal development of the applications. The results of risk analyses performed at the information technology installation where the applications will be processed should be taken into account when defining and approving security

specifications for the applications. Other vulnerabilities of the applications, such as in telecommunications links, shall also be considered in defining security requirements. The views and recommendations of the information technology user organization, the information technology installation, and the individual responsible for security at the installation shall be considered prior to the approval of security specifications for the applications.

(b) Design Reviews and System Tests. Agencies shall conduct and approve design reviews and system tests, prior to placing the application into operation, to assure the proposed design meets the approved security specifications. The objective of the system tests should be to verify that required administrative, technical, and physical safeguards are operationally adequate. The results of the design reviews and system tests shall be fully documented and maintained in the official agency records.

(c) Certification. Upon completion of the system tests, an agency official shall certify that the system meets all applicable Federal policies, regulations, and standards, and that the results of the tests demonstrate that the installed security safeguards are adequate for the application.

(2) Periodic Review and Recertification. Agencies shall conduct periodic audits or reviews of sensitive applications and recertify the adequacy of security safeguards. Audits or reviews shall evaluate the adequacy of implemented safeguards, assure they are functioning properly, identify vulnerabilities that could heighten threats to sensitive data or valuable resources, and assist with the implementation of new safeguards where required. They are intended to provide a basis for recertification of the security of the application. Recertification shall be fully documented and maintained in the official agency records. Audits or reviews and recertifications shall be performed at least every three years. They should be considered as part of agency vulnerability assessments and internal control reviews conducted in accordance with OMB Circular No. A-123. Security or other control weaknesses identified shall be included in the annual internal control assurance letter and report required by Circular No. A-123.

(3) Contingency Plans. Agencies shall establish policies and assign responsibilities to assure that appropriate contingency plans are developed and maintained by end users of information technology applications. The intent of such plans is to assure that users can continue to perform essential functions in the event their information technology support is interrupted. Such plans should be consistent with disaster recovery and continuity of operations plans maintained by the installation at which the application is processed.

b. Personnel Security. Agencies shall establish and manage personnel security policies and procedures to assure an adequate level of security for Federal automated information systems. Such policies and procedures shall include requirements for screening all individuals participating in the design, development, operation, or maintenance of sensitive applications as well as those having access to sensitive data. The level of screening required by these policies should vary from minimal checks to full background investigations, depending upon the sensitivity of the information to be handled and the risk and magnitude of loss or harm that could be caused by the individual. These policies shall be established for both Federal and contractor personnel. Personnel security policies for Federal employees shall be consistent with policies issued by the Office of Personnel Management.

c. Information Technology Installation Security. Agencies shall assure that an appropriate level of security is maintained at all information technology installations operated by or on behalf of the Federal Government (e.g., government-owned, contractor-operated installations).

(1) Assigning Responsibility. Agencies shall assign responsibility for the security of each installation to a management official knowledgeable in information technology and security matters.

(2) Periodic Risk Analysis. Agencies shall establish and maintain a program for the conduct of periodic risk analyses at each installation to ensure that appropriate, cost effective safeguards are incorporated into existing and new installations. The objective of a risk analysis is to provide a measure of the relative vulnerabilities and threats to an installation so that security resources can be effectively distributed to minimize potential loss. Risk analyses may vary from an informal review of a microcomputer installation to a formal, fully quantified risk analysis of a large scale computer system. The results of these analyses should be documented and taken into consideration by management officials when certifying sensitive applications processed at the installation. Such analyses should also be consulted during the evaluation of general controls over the management of information technology installations conducted in accordance with OMB Circular No. A-123. A risk analysis shall be performed:

(a) Prior to the approval of design specifications for new installations;

(b) Whenever a significant change occurs to the installations (e.g., adding a local area network; changing from batch to online processing; adding dial-up capability). Agency criteria for defining significant change shall be commensurate with the sensitivity of the data processed by the installation.

(c) At periodic intervals established by the agency commensurate with the sensitivity of the data processed, but not to exceed every five years if no risk analysis has been performed during that period.

(3) Disaster and Continuity Plan. Agencies shall maintain disaster recovery and continuity of operations plans for all information technology installations. The objective of these plans should be to provide reasonable continuity of data processing support should events occur that prevent normal operations at the installation. For large installations and installations that support essential agency functions, the plans should be fully documented and operationally tested periodically, at a frequency commensurate with the risk and magnitude of loss or harm that could result from disruption of information technology support.

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

d. Security Awareness and Training Programs. Agencies shall establish a security awareness and training program to assure that agency and contractor personnel involved in the management, operation, programming, maintenance, or use of information technology are aware of their security responsibilities and know how to fulfill them. Users of information technology systems should be apprised of the vulnerabilities of such systems and trained in techniques to enhance security.

#### 4. Assignment of Responsibilities

a. Department of Commerce. The Secretary of Commerce shall:

(1) Develop and issue standards and guidelines for assuring the security of Federal automated information systems;

(2) Establish standards, approved in accordance with applicable national security directives, for systems used to process sensitive information the loss of which could adversely affect the national security interest; and

(3) Provide technical assistance to Federal agencies in implementing Department of Commerce standards and guidelines.

b. Department of Defense. The Secretary of Defense shall:

(1) Act, in accordance with applicable national security directives, as executive agent of the government for the security of telecommunications and automated information systems that process information the loss of which could adversely affect the national security interest; and

(2) Provide technical material and assistance to Federal agencies concerning security of Federal telecommunications and automated information systems.

c. General Services Administration. The Administrator of General Services shall:

(1) Issue policies and regulations for the physical and environmental security of computer rooms in Federal buildings consistent with standards issued by the Department of Commerce and the Department of Defense.

(2) Assure that agency procurement requests for computers, software, telecommunications services, and related services include security requirements. Delegations of procurement authority to agencies by GSA under mandatory programs, dollar threshold delegations, certification programs, or other so-called blanket delegations shall include requirements for agency specification of security requirements.

(3) Assure that information technology equipment, software, computer room construction, guard or custodial services, telecommunications services, and any other related services procured by GSA meet the security requirements established and specified by the user agency and are consistent with other applicable policies and standards issued by OMB, the Department of Commerce, the Department of Defense, and the Office of Personnel Management.

(4) Issue appropriate standards for the security of Federal telecommunications systems. Standards related to systems used to communicate sensitive information, the loss of which could adversely affect the national security interest, shall be developed and issued in accordance with applicable national security directives.

d. Office of Personnel Management. The Director, Office of Personnel Management, shall maintain personnel security policies for Federal personnel associated with the design, programming, operation, maintenance, or use of Federal automated information systems. Requirements for personnel checks imposed by these policies should vary commensurate with the risk and magnitude of loss or harm that could be caused by the individual. The checks may range from merely normal reemployment screening procedures to full background investigations.

92

## 5. Reports

In their annual internal control report to the President and the Congress, required under OMB Circular No. A-123, agencies shall:

- a. Describe any security or other control weaknesses identified during audits or reviews of sensitive applications or when conducting risk analyses of installations; and
- b. Provide assurance that there is adequate security of agency automated information systems.

APPENDIX IV  
TO OMB CIRCULAR NO. A-130  
-  
ANALYSIS OF KEY SECTIONS

1. Purpose

The purpose of this Appendix is to provide a general context and explanation for the contents of the key sections of the Circular.

2. Background

The Paperwork Reduction Act of 1980, P.L. 96-511, 94 Stat 2812, codified at Chapter 35 of Title 44 of the United States Code, establishes a broad mandate for agencies to perform their information activities in an efficient, effective, and economical manner. Section 3504 of the Act provides authority to the Director, Office of Management and Budget (OMB), to develop and implement uniform and consistent information resources management policies; oversee the development and promote the use of information management principles, standards, and guidelines; evaluate agency information management practices in order to determine their adequacy and efficiency; and determine compliance of such practices with the policies, principles, standards, and guidelines promulgated by the Director.

The Circular implements OMB authority under the Act with respect to Section 3504(b), general information policy, Section 3504(e), records management, Section 3504(f), privacy, and Section 3504(g), Federal automatic data processing and telecommunications; the Privacy Act of 1974 (5 U.S.C. 552a); Sections 111 and 206 of the Federal Property and Administrative Services Act of 1949, as amended (40 U.S.C. 759 and 487, respectively); the Budget and Accounting Act of 1921 (31 U.S.C. 1 et seq.); and Executive Order No. 12046 of March 27, 1978 and Executive Order No. 12472 of April 3, 1984, Assignment of National Security and Emergency Telecommunications Functions. The Circular complements 5 CFR 1320, Controlling Paperwork Burden on the Public, which implements other sections of the Paperwork Reduction Act dealing with controlling the reporting and recordkeeping burden placed on the public.

In addition, the Circular revises and consolidates policy and procedures in five existing OMB directives and rescinds those directives, as follows:

A-71 - Responsibilities for the Administration and  
Management of Automatic Data Processing Activities

Transmittal Memorandum No. 1 to Circular No. A-71 - Security  
of Federal Automated Information Systems

A-90 - Cooperating with State and Local Governments to  
Coordinate and Improve Information Systems

A-108 - Responsibilities for the Maintenance of Records  
about Individuals by Federal Agencies

A-121 - Cost Accounting, Cost Recovery, and Interagency  
Sharing of Data Processing Facilities

OMB's review of the five existing policy directives led to the conclusion that much, but not all, of their content was procedural in nature, concerned chiefly with how policies were to be carried out. OMB determined that it was important clearly to distinguish the statement of policies from the procedures for implementing those policies. For this reason, the main body of the Circular consists of basic considerations and assumptions, policies, and assignments of responsibility; the appendices to the Circular consist of procedures for implementing various policies and with analysis of key sections.

OMB developed the main body of the Circular relying upon comments on the Federal Register notice as well as other forms of Federal agency and public input, principally meetings with interested parties. For the procedural revisions, OMB relied on the assistance of interagency task groups.

The revised contents of OMB Circular No. A-71, dealing with assignments of responsibilities, are in the main body of this Circular. The contents of OMB Circular No. A-90 are rescinded entirely, with the exception of a policy statement at Section 3 (b)(17) of this Circular. Revisions of the procedural aspects of the other three policy directives--Transmittal Memorandum No. 1 to A-71, A-108, and A-121--are appendices to this Circular. Appendices I, II, and III have the same prescriptive force as the Circular; Appendix IV is an explanatory document.

On September 17, 1984, the President signed National Security Decision Directive (NSDD) No. 145, National Policy on Telecommunications and Automated Information Systems Security. The NSDD requires that the Director, OMB, review for consistency with the NSDD, and amend as appropriate, OMB Circular No. A-71, Transmittal Memorandum No. 1. The Circular and Appendix III satisfy the NSDD requirement.

### 3. Analysis

#### Section 6. Definitions

f. Access to information. g. Dissemination of information. The Circular defines "access to information" as the function of providing to members of the public, upon their

request, the government information to which they are entitled under law. Access refers to those situations in which the government agency's role is passive; access is what the government's responsibilities are when the public comes to the government and asks for information the government has and the public is entitled to. "Dissemination," in the Circular's usage, refers to the function of distributing government information; dissemination connotes an active outreach by a government agency. Dissemination refers to those situations in which the government provides the public with information without the public having to come and ask for it.

The distinction between access and dissemination is posed in order to elaborate the responsibilities of Federal agencies for providing information to the public. Two fundamentally different situations exist: one in which the public goes to the agency to ask for information the agency holds and may or may not have disseminated; and one in which the agency chooses to take the information it holds to the public. In the first instance--access--Congress has provided specific statutory policy in the Freedom of Information Act (FOIA) and in the Privacy Act. These laws and policies concerning access to government information are explicit, well known, and now so widely accepted in practice by Federal agencies as not to require policy elaboration in this Circular. Agencies should know that, if members of the public ask for information subject to FOIA or the Privacy Act, the agencies should normally provide the information forthwith, because the public has a formal legal process for forcing the agencies to yield the information.

The relationship between access to and dissemination of information is explained below, in the discussion of 8a(8) through (12).

#### Section 7. Basic Considerations and Assumptions

Basic considerations and assumptions are statements that provide the underpinnings for the prescriptive policies in Section 8; they are not themselves policy statements. They are either derived from statutes or legislative history, or represent executive branch management philosophy as embodied in the Circular.

- Statements 7-a through 7-d provide the general context for management of Federal information resources.
- Statement 7-e summarizes policy found in OMB Circular No. A-76, Performance of Commercial Activities.
- Statement 7-f states a general predisposition to use up-to-date information technology to manage Federal information resources.

- Statements 7-g and 7-h pertain to the Privacy Act and the Freedom of Information Act, respectively.
- Statement 7-i pertains to the National Science and Technology Policy, Organization and Priorities Act.
- Statement 7-j pertains to the Federal Records Act.
- Statement 7-k states a relationship between Federal information policy and international information policy.

### Section 8. Policies.

This section is divided into two subsections that generally correspond to the twofold definition of information resources management in Section 6-b, namely, information itself and the resources associated with information.

a. Information Management. The Paperwork Reduction Act acknowledges that information is a valuable resource and should be managed as such. Proceeding from this premise, this subsection states policies concerning the management of Federal information.

(1) and (2). Information Collection and Sharing. The Circular's basic considerations and assumptions (Section 7) establish the value of government information activities. Without question, some information created or collected by Federal agencies is so vital that the American form of government, the economy, national security, and citizens' safety and wellbeing could not continue to exist in its absence. Nothing in this Circular is intended to diminish or derogate the creation or collection of such information, nor to serve as a pretext under which a Federal agency could damage the Nation's critical needs by failing to create or collect such information.

At the same time, the Paperwork Reduction Act was designed to remedy deficiencies Congress perceived in Federal information activities. In the words of the report of the House Committee on Government Operations (Report No. 96-835, p. 3):

The legislation is the result of a growing concern that the way the Government collects, uses, and disseminates information must be improved. Inefficiencies in current Federal information practices drastically reduce the effectiveness of the Government while, at the same time, drowning our citizens in a sea of forms, questionnaires, and reports.

The Act intends that the creation or collection of information be carried out within the context of efficient, effective, and economical management. When Federal agencies create or collect

information--just as when they perform any other vital functions --they consume scarce resources and such activities must be continually scrutinized in light of good management principles. The applicable principles provided in the purposes of the Act are:

- to minimize the Federal paperwork burden for individuals, small businesses, State and local governments, and other persons;
- to minimize the cost to the Federal Government of collecting, maintaining, using, and disseminating information; and
- to maximize the usefulness of information collected by the Federal Government. (44 U.S.C. 3501)

Agencies must justify the creation or collection of information in the light of their statutory functions. Policy statement 8a(9) uses the standard, "necessary for the proper performance of agency functions," taken directly from the Paperwork Reduction Act (44 U.S.C. 3504 (c)(2)). Further, the policy statement includes the requirement that the information have practical utility, as defined in the Paperwork Reduction Act (44 U.S.C. 3502 (15)) and elaborated in Controlling Paperwork Burdens on the Public (5 CFR 1320). Note that practical utility includes characteristics pertaining to the quality of information such as accuracy, adequacy, and reliability, and that, in the case of general purpose statistics or recordkeeping, practical utility means that actual uses can be demonstrated (5 CFR 1320.7 (q)).

Good management and the requirement of practical utility dictate that agencies must plan from the outset for the steps in the information life cycle. The Act also stipulates that agencies must "formulate plans for tabulating the information in a manner which will enhance its usefulness to other agencies and to the public" (44 U.S.C. 3507 (a)(1)(C)). When creating or collecting information, agencies must plan how they will process and transmit the information, how they will use it, what provisions they will make for access to it, whether and how they will disseminate it, how they will store it, and finally, how the information will ultimately be disposed of. While agencies cannot at the outset achieve absolute certitude in planning for each of these processes, the requirement for information resources planning is clearly contained in the Act (44 U.S.C. 3506 (c)(1)), and the absence of adequate planning is sufficient reason not to create or collect information in the first place.

Before creating or collecting new information, agencies should look first to other agencies and the private sector so as not to duplicate existing information sources or services that would satisfy their needs. The Act requires that agencies shall not conduct or sponsor information collections unless they have eliminated collections "which seek to obtain information

available from another source within the Federal Government" (44 U.S.C. 3507 (a)(1)(A)). Each agency must also "ensure its information systems do not overlap each other or duplicate the systems of other agencies" (44 U.S.C. 3506 (c)(2)). The Act also contains provisions governing the sharing of information between agencies (44 U.S.C. 3510). Applying the policy of OMB Circular No. A-76, the Circular also requires agencies to examine the possibility of acquiring the necessary information from private sector sources.

This is not to say that information creation or collection functions should be indiscriminately turned over to other agencies or to the private sector, but rather to say that agencies have an obligation to examine other potential sources of information which may satisfy agency needs. Some information can only be created or collected by Federal agencies themselves in the exercise of the government's sovereign powers. For some information, the government can satisfy its legitimate needs only when a Federal agency is the creation or collection agent. But other information needs can be met, and in many cases are routinely met, through existing services and sources in other agencies or the private sector. In many cases there is no inherently governmental function that is served by having information collected by a Federal agency; agencies should and do consider acquiring information collection services from the private sector. The Circular emphasizes that these sources should always be looked to first in the interests of efficiency and economy.

(3) through (6). Privacy Act and Freedom of Information Act. These statements contain policy statements pertaining to the Privacy Act and incorporating the policies of OMB Circular No. A-108, which is rescinded and superseded. Agencies are to ensure that they meet the requirements of the Privacy Act regarding collection of individually identifiable information. Such information is to be maintained and protected so as to preclude intrusion into the privacy of individuals. Individuals must be accorded access and amendment rights to records, as provided in the Privacy Act. Appendix J prescribes procedures for the maintenance of records about individuals in accordance with the Privacy Act.

In addition to Privacy Act considerations, statements (3) and (4) include provisions concerning proprietary information. Agencies are to minimize their collection of proprietary information, consistent with legal requirements and operational necessity and, when such information must be collected, agencies must provide for its protection.

(7). Training. Agency personnel must receive proper training to safeguard information resources. Training is particularly important in view of the changing nature of information resources management. The development of end user computing and office automation, for example, place the

management of information and information technology in the hands of nearly all agency personnel rather than in the hands of a few employees at centralized facilities such as large computer centers. Policies and procedures for computer security, records management, protection of privacy, and other safeguards need to be incorporated into information resources management training programs.

(8) through (12). Information Dissemination.

(8) and (9). General Policy. How does the public know what information is available from Federal agencies? That is, given the distinction the Circular makes between access and dissemination, what is the relationship between the two? How does the public know what government information is accessible? The answer is: through the government's dissemination of information on what is available and how to gain to access it.

The Freedom of Information Act requires each agency to publish currently in the Federal Register, for the guidance of the public, descriptions of agency organization; where and how the public may obtain information; the general course and methods by which agency functions are determined, including all procedural requirements; rules of procedure; descriptions of forms and how to obtain them; substantive regulations; statements of general policy; and revisions to all the foregoing (5 U.S.C. 552 (a)(1)). The Privacy Act also requires publication of information concerning systems of records (see Appendix I); the Government in the Sunshine Act requires agencies to make public announcement of meetings (5 U.S.C. 552b (e)(1)). The Paperwork Reduction Act (44 U.S.C. 3507 (a)(2)) and Controlling Paperwork Burdens on the Public (5 CFR 1320) require agencies to publish notices when they submit information collection requests for OMB approval.

In sum, every Federal agency has obligations to disseminate basic information to the public concerning what the agency does, how its programs operate, what the public must do to comply with laws or regulations, how to receive benefits, and how the public can use agency services. These obligations are the basic linkage between access to, and dissemination of, government information.

Beyond generic requirements, specific laws affect agency dissemination of information in two ways. First, for some agencies their basic enabling legislation stipulates that information dissemination is part of their statutory mission. General purpose statistical agencies, for example, have information dissemination as part of their very reason for existence. These agencies conduct substantial information dissemination programs in order to carry out their necessary functions. In contrast, other agencies such as some regulatory agencies have basic information access, but minimal information dissemination responsibilities; the existence of substantial information dissemination programs in such agencies would be

unusual. Second, statutes may sometimes require that agencies produce and disseminate specific information products or services. For example, the law may state that the President or head of an agency shall make reports to the Congress on given subjects; these would be legally required disseminations of information.

Beyond generic and specific statutory requirements, agencies have positive obligations to disseminate information as a necessary part of performing their functions. Each agency head must clarify the nature of these obligations for the agency's particular mission and set appropriate boundaries for dissemination functions. Before deciding to disseminate an information product or service, and periodically thereafter, an agency must be able to demonstrate that the dissemination of the product or service passes the test of either being required by law or being necessary for the proper performance of agency functions.

In conformity with the purposes of the Paperwork Reduction Act, the agency's positive obligations to disseminate information must be discharged within a responsible management framework of minimizing costs to the Federal Government while maximizing the usefulness of the information. Efficient, effective, and economical dissemination does not translate into diminishing or limiting the flow of information from the agency to the public. To the contrary, good management of information resources should result in more useful information flowing with greater facility to the public, at less cost to the taxpayer.

Given an adequate basis for dissemination, agencies must also ask themselves whether a proposed or existing information product or service substantially duplicates similar products or services that would otherwise be available, either from another agency or from the private sector. This requirement of non-duplication, originating in the Paperwork Reduction Act, husbands scarce resources and leads to more efficient, effective, and economical information dissemination by the government.

Similarly, the fact that an agency has created or collected information is not itself a valid reason for creating a program, product, or service to disseminate the information to the public. Agencies create and collect much information, often for purely internal governmental purposes, that is not intended for dissemination, for which there is no public demand, and the dissemination of which would serve no public purpose and would not be cost-justified; e.g., compilations of routine time and attendance records for Federal employees, or publication of the thousands of pages of common carrier tariff filings by regulatory agencies. While such information may be subject to access upon request under provisions of agency statutes, the Freedom of Information Act, or the Privacy Act, the agency must demonstrate in each case the need actively to disseminate such information. Over time, changes in laws, economic conditions, or information

technology can result in changes in public demand, public purpose, or dissemination costs; for example, an agency's shift to electronic filing of reports, perhaps carried out primarily in order to improve internal information management, might generate a public demand for electronic dissemination that could be satisfied at minimal cost to the government and also improve the performance of the agency's information access function. The decision to disseminate information, however, entails potentially significant costs, must be addressed separately from the decision to create or collect information, and must hinge upon a determination that dissemination is necessary for proper performance of agency functions.

If agencies do contemplate disseminating particular information, they should plan for its dissemination when creating or collecting the information (see 8a(1)). Planning for dissemination should proceed from the Paperwork Reduction Act premises of minimizing the cost to the government while maximizing the usefulness of information. The focus of information dissemination plans should be on elevating to a policy level decisions regarding the agency's positive obligations to disseminate information and ensuring that the agency discharges the obligations in the most efficient, effective, and economical manner.

(10) Adequate Notice. Because many government information activities are important to the government and to the public, agencies must exercise care not to act capriciously with respect to information products and services. When agencies intend to commence offering new products or services, they should provide adequate advance notice so that the public may comment as to the need for the product or service. For example, if private sector interests believe they are already offering or are about to offer the same or a similar product or service--in which event the government may potentially be entering into unfair competition--such notice will allow these interests to present their case before the product or service is launched. By the same token, if many members of the public greatly depend on a particular product or service, they should be permitted to voice their views to an agency that is contemplating termination of the product or service.

The Circular refers to "significant" information products and services. It is not the Circular's intent that agencies should follow notice and comment procedures when terminating relatively inconsequential information products and services; examples might be minor brochures or flyers, products and services that were never intended to be continuing, or for which there is now little or no public audience. Agencies should determine for themselves whether information products and services are "significant," and in some cases may wish to establish procedures and threshold criteria for making such determinations. If a product or service

is considered significant, as determined ultimately by the agency head, the agency may be well advised to follow notice and comment procedures prior to initiation or termination.

(11)(a). Reaching the Public; Avoiding Information Monopolies. When agencies have justified and made the basic decision to disseminate information, they must also satisfy conditions regarding the manner of dissemination. First, agencies must take steps to ensure that members of the public whom the agency has an obligation to reach have a reasonable ability to acquire the information. The audiences for information products and services will vary, and agencies should tailor the dissemination methods so as to place the information into the hands of those whom the agency intends to receive it.

Federal agencies are often the sole holders of certain information; hence, when they disseminate, they are sole suppliers and in a position of natural monopoly. When agencies use private sector contractors to accomplish dissemination, they must take care that they do not permit contractors to exercise monopolistic controls in ways that defeat the agencies' information dissemination obligations, for example, by setting unreasonably high prices. In some cases agencies may need to formulate contractual terms with a sole supplier contractor so that the contractor functions as a mere intermediary for the agency in dealing with end users in the public.

(11)(b). Reliance on the Private Sector. In disseminating information--as with other activities--agencies must act in the most cost effective manner, which includes maximum feasible reliance on the private sector. This is merely an application to agency information dissemination programs of the policy stated in OMB Circular No. A-76, Performance of Commercial Activities, and summarized in Section 7f of this Circular. It is "the general policy of the government to rely on commercial sources to supply the products and services the government needs," including products and services the government needs in order to disseminate information to the public. For example, before an agency establishes a service for electronic dissemination of government information via an online computer system, the agency should compare the cost of contracting for operation of the service versus in-house performance and determine whether in-house performance is less costly both for the government and for the public who will receive the service.

Policies contained in OMB Circular No. A-76 are applicable to information dissemination, including the policy that inherently governmental functions should be performed by government employees. The general policy of reliance on the private sector is balanced by the "inherent governmental function" policy, and the Circular in no way intends to abrogate the latter. Where agencies determine that information dissemination activities are inherently governmental, the agencies themselves should carry out the activities.

(11)(c). User Charges. The Federal Government is the sole possessor and supplier of certain types of information, which is frequently of substantial commercial value. Dissemination of such information, or its dissemination in a specific form or medium, may represent a government service from which identifiable recipients derive special benefits, in which case they may be subject to OMB Circular No. A-25, User Charges. For example, where the information is already substantially available in printed form, agencies may consider dissemination in electronic form to be a service of special benefit, the costs of which should be recovered through user charges. Many agencies do not have consistent, agency-wide policies and procedures for setting user charges for information products and services with a view to cost recovery. Agencies must establish user charges for the costs of information dissemination, and recover such costs, where appropriate. Whether user charges are appropriate depends, in principle, on whether identifiable recipients will receive special benefits from information products and services.

The requirement to establish user charges is not, however, intended to make the ability to pay the sole criterion for determining whether the public receives government information. Agencies must balance the requirement to establish user charges and the level of fees charged against other policies, specifically, the proper performance of agency functions and the need to ensure that information products and services reach the public for whom they are intended (see Section 8a (11)(a)). If an agency has a positive obligation to place a given product or service in the hands of certain specific groups or members of the public and also determines that user charges will constitute a significant barrier to discharging this obligation, the agency may have grounds for reducing or eliminating its user charges for the product or service, or for exempting some recipients from the charge.

(12). Periodic Review and Depository Libraries. Agencies must also establish procedures for periodically reviewing their information dissemination programs. Agency information dissemination plans must ask whether the agency should disseminate a given information product or service at all; if the agency is already disseminating the product or service, reviews should ask whether the agency should continue to do so; or whether the manner or medium of dissemination is the most efficient, effective, and economical.

In addition, agencies must establish procedures to ensure compliance with 44 U.S.C. 1902, which requires that government publications (defined in 44 U.S.C. 1901 and repeated in Section 6k of the Circular) be made available to the Federal depository libraries through the Government Printing Office. The depository libraries provide a kind of information "safety net" to the public, an existing institutional mechanism that guarantees a minimum level of availability of government information to all

members of the public. Providing publications to the depository library program complies with the law and costs executive agencies virtually nothing.

b. Information Systems and Information Technology Management. This subsection states policies concerning the planning, acquisition, operation, and management of Federal information systems and technology. The Federal information systems and technology budget, which was \$14 billion in FY 1985, is projected to increase at a rate faster than that of the overall Federal budget. With outlays at these levels and agencies becoming increasingly dependent upon information technology to accomplish their missions, it is essential that planning processes be applied to the acquisition and application of information technology.

(1). Planning. The Paperwork Reduction Act mandates a stronger central role in information resources planning. Specifically, the Act requires that OMB: (1) publish a five-year government-wide automatic data processing and telecommunications plan; (2) review and coordinate agency proposals for the acquisition and use of information technology; and (3) promote the use of the technology to improve governmental efficiency and effectiveness. In order to meet these objectives, it is necessary to initiate a government-wide process for developing and institutionalizing information technology planning that is based in agency programs and missions. The planning must also be tied to the budget so that budgetary decisions derive from plans, and conversely, so that budgetary constraints are reflected in the plans. The process must further ensure that sufficient information is available to the central agencies to enable them to monitor compliance with Federal policies and identify major issues, including cross-cutting issues where more active centralized planning and management may be appropriate. Hence, agencies must institute information planning processes tied to both the conduct of programs and the preparation of the agency's budget.

(2) and (3). Management Controls and Accountability. Basic management controls for agency information systems are fundamental to sound information resources management. These controls should ensure the documentation and periodic review of major information systems, as well as periodic cost-benefit evaluation of overall information resources management in light of agency missions. In order to provide greater incentive for management efficiencies, accountability for information systems should be vested in the officials responsible for operating the programs that the systems support.

Program managers depend upon information systems to carry out their programs, and yet frequently they do not have direct control over the technical and operational support for those systems. Program managers often depend upon agency computer centers or contracted service organizations, the heads of which

may not be directly accountable to the program managers in a formal organizational sense. Program managers are nonetheless responsible for conducting their programs and, to the extent successful conduct of the programs entails support from information systems, program managers must be held accountable for acquiring that support. The responsibilities of program managers are therefore presumed to include securing information systems support as needed, and planning for contingencies. Technical support organizations have a concomitant responsibility to meet their commitments, contractual or otherwise, to their program clients, but the program official has the ultimate responsibility for delivering a program's product or service.

(4) and (5). Sharing Information Processing Capacity  
OMB Circular No. A-121, which is rescinded and superseded, required only that the holder of excess automatic data processing capacity share such capacity. Because the holder of excess capacity has little incentive to seek opportunities for sharing, however, the new policy requires both that the holder share capacity and that the agency seeking information processing capacity fulfill its needs from other agencies or the private sector, whenever possible, before acquiring the new capacity itself. The policy establishes an order of preference in meeting needs--look first to existing sources before acquiring new capacity--but is not intended to assert blindly that sharing or commercial sources are the sole considerations. Agencies must also consider whether existing sources are more cost effective and whether they in fact will meet agency specific needs. Procedural aspects of these policy statements are found in Appendix II.

(6) and (7). Life Cycle Costing; and Avoiding Duplication. Agencies frequently develop information technology incrementally, through a series of interim upgrades, without regard for longer term considerations such as the information systems' life cycle. As part of their planning, agencies need to consider the full information system life cycle when determining the cost of information technology. While competitive procurement is generally to be valued, its costs should be taken into account, including the cost to program effectiveness of unnecessarily lengthy procurement processes. Other conditions, such as the need for compatibility, may also be legitimate limitations on the competitive process. Similarly, agency planning should ensure that information systems are not unnecessarily duplicative of systems available elsewhere in government or from the private sector.

(8). Software Management. The prevailing agency practice of developing customized computer software is a source of inefficiency, as the General Accounting Office and others have noted. While some agency applications can only be satisfied with customized software, the tendency to prefer custom development is excessively costly in terms of initial development, continued maintenance, and eventual conversion to new technology, because

it requires the agency to bear the full cost of developing and maintaining the software it uses. While recognizing that off-the-shelf software has pitfalls, such as uncertainty of continued maintenance, managers are generally to prefer acquiring generic, off-the-shelf software available from the private sector instead of developing their own.

(9). Necessary Compatibility. Agencies often acquire technology that is incapable of communicating with other systems with which the agencies need to communicate. Compatibility among information systems has consequently emerged as a significant information resources management problem. Agencies must acquire or develop information systems in a manner that enhances necessary compatibility. The qualifier "necessary" is used because compatibility is not an unrestricted goal; information systems need to be compatible with other systems only to the extent that they must communicate with those systems.

(10) through (13). Security. Security of information systems means both the protection of information while it is within the systems and also the assurance that the systems do exactly what they are supposed to do and nothing more. Information system security entails management controls to ensure the integrity of operations including such matters as proper access to the information in the systems and proper handling of input and output. In this sense, security of information systems is first and foremost a management issue and only secondly a technical problem of computer security.

The recent introduction of smaller and more powerful computer systems and new communications technology and transmission media, together with the greater involvement of end users in managing information resources, have increased the potential vulnerability of Federal information systems and hence the level of management concern. Protecting personal, proprietary, and other sensitive data from unauthorized access or misuse; detecting and preventing computer related fraud and abuse; and assuring continuity of operations of major information systems in the event of emergency related disruptions are increasingly serious policy issues. Policy previously found in Transmittal Memorandum No. 1 to OMB Circular No. A-71 is here revised; procedural aspects of the policy are in Appendix III to the Circular.

The General Accounting Office reported in its review of the first-year implementation of the Federal Managers Financial Integrity Act (FIA) that internal controls in automatic data processing systems received inadequate coverage in FIA evaluations. GAO noted that some agencies were uncertain of the relationship between (a) OMB Circular No. A-71, Transmittal Memorandum No. 1, Security of Federal Automated Information Systems, and (b) OMB Circular No. A-123, Internal Control Systems. The relationship between security of automated information systems and agency internal control reports is now stated clearly in Appendix III.

Appendix III provides a minimal set of requirements for the security of all Federal automated information systems. The Appendix also requires agencies to incorporate additional requirements for the security of information classified for national security purposes, in accordance with appropriate national security directives.

(14). Standards. The National Bureau of Standards, Department of Commerce, develops and issues Federal Information Processing Standards. The National Communications System develops and the General Services Administration issues Federal Telecommunications Standards. Some standards are mandatory for Federal agencies, while others are voluntary. Agencies may waive the use of Federal standards under certain conditions and pursuant to certain procedures, which vary depending upon the individual standard. In general, OMB strongly recommends use of these standards government-wide. Such standards can contribute to overall government economy and efficiency by increasing compatibility in computer and telecommunications networks, improving the transportability of software, and enabling computer systems to be developed using components of different manufacturers. These advantages can result in reduced procurement costs for equipment and services, improved competition, and better utilization of staff training and skills. While government-wide standards can result in management efficiencies, agencies should be mindful that standards can also have the untoward effects of regulations, as noted in OMB Circular No. A-119. Agencies should continuously assess relative costs and benefits of standards and their effects upon the agency's accomplishment of its mission. Note also that national security directives prescribe standards for computer security.

(15) Avoiding Information Technology Monopolies. Many agencies operate one or more central information technology facilities to support agency programs. In these agencies, program managers are often required to use the central facilities. The manager of such a monopoly facility has a lesser incentive to control costs, since he or she has a captive clientele. The program manager has little leverage to ensure that information processing resources are efficiently allocated since he or she cannot seek, or can seek only with great difficulty, alternative sources of supply. When users are dependent on effective technology support to perform their functions, control over selection of facility is essential and consistent with holding users responsible for producing their government information products. To provide incentives conducive to more businesslike procedures in information technology facilities, agencies should avoid monopolistic information processing arrangements and should enter into them only if their cost effectiveness is clear and they are subject to periodic review. Appendix II specifies certain procedures with respect to this policy.

126

(16) Cost Recovery. This policy constitutes a revision to policy stated in OMB Circular No. A-121. Whereas Circular No. A-121 required only that costs for automatic data processing facilities be allocated to users, agencies must now recover the costs of information technology facilities from government users. Viable management of a large information technology facility requires that managers know the amount of resources devoted to each user when providing services. Furthermore, effective management of the use of information technology requires that the user have responsibility for and control over the resources consumed by use of the facility. Experience with Circular No. A-121 showed OMB that allocating costs had little effect on agencies' behavior; recovering costs means that actual transfers of funds will take place between suppliers and users of information technology facilities. Procedural aspects of the policy appear in Appendix II.

(17) Coordination with State and Local Governments. This policy reaffirms policy previously found in OMB Circular No. A-90, Transmittal Memorandum No. 1. The interagency group that worked on the revision of Circular No. A-90 recommended, and OMB agreed, that the Circular should be rescinded except for a single policy statement prohibiting Federal agencies from placing unnecessary restrictions on the information systems that State and local governments use to carry out federally financed program activities.

(18) Application of Up-to-date Information Technology. Recent availability of low cost, highly efficient and effective electronic information technology can greatly increase worker productivity and facilitate operation of Federal agency programs. The Circular states a predisposition, based in the Paperwork Reduction Act, in favor of applying such technology to the information life cycle within a responsible management context. Two broad areas of information technology merit further discussion: (1) electronic information collection and dissemination, and (2) end user computing.

- Electronic Collection and Dissemination of Information. Federal agencies are moving rapidly to provide for collection and dissemination of information through electronic media. In developing this Circular, OMB considered whether it was necessary to provide specific policies concerning electronic collection and dissemination of governmental information. OMB concluded that, except for the general predisposition in favor of applying new technological developments to information resources management, the policies that apply to information collection and dissemination in other media also apply to electronic collection and dissemination. It is important, however, that agencies recognize the necessity of systematically thinking through the application of policies stated elsewhere in this Circular to electronic collection and dissemination of information. For example, when developing electronic collection programs, agencies

should give particular attention to issues such as privacy, public access, and records management. When developing electronic dissemination programs, agencies should ensure that access is provided to each class of users upon reasonable terms, avoid problems arising from monopolistic control, ensure maximum reliance upon the private sector, and take necessary steps for cost accounting and cost recovery:

- End User Computing. Federal agencies are also moving rapidly to acquire end user computing capabilities. OMB endorses the managed innovation approach to end user computing presented in GSA's publication Managing End User Computing in the Federal Government (June 1983). Because end user computing places management of information in the hands of individual agency personnel rather than in a central automatic data processing organization, the Circular requires that agencies train end users in their responsibilities for safeguarding information; Appendix III deals in part with the security of end user computing.

### Section 9. Assignment of Responsibilities.

This section assigns responsibilities for the management of Federal information resources addressed in this Circular. OMB Circular No. A-71 is rescinded and its contents are revised and incorporated into this section along with responsibilities assigned under the Paperwork Reduction Act; Section 111 of the Federal Property and Administrative Services Act, as amended; and Executive Order No. 12046. Certain assignments of responsibility from OMB to other agencies, as noted below, are also included. Following are principal noteworthy aspects of this section.

#### Responsibility for Managing Information Resources.

Statement 9a(1) is a key element in the Circular because it establishes that the locus of responsibility for actual management of Federal information resources is the head of each agency. This means, for example, that the determination of what is "necessary for the proper performance of agency functions" with respect to information creation or collection (8a(1)) and information dissemination (8a(9)) lies with the head of the agency. In the Circular OMB sets the policy framework within which such determinations are to be made and the standards and provisions for reviewing the determinations, but the management decisions and their implementation belong properly with the agency holding the information resources.

Triennial Reviews. The Paperwork Reduction Act provides that the Director of OMB ". . . shall, with the advice and assistance of the Administrator of General Services, selectively review, at least once every three years, the information management activities of each agency to ascertain their adequacy and efficiency." (44 U.S.C. 3513) The Administrator of Information and Regulatory Affairs, OMB, and the Deputy Administrator of the General Services Administration, in an

exchange of correspondence dated June 13 and July 22, 1983, concurred that GSA has the necessary statutory authority to conduct reviews of Federal agency information resources management activities. Separate triennial reviews of agency activities by OMB and GSA would be unnecessarily duplicative, which would not be consistent with the Act. Accordingly, the triennial reviews conducted by GSA will be designed to meet OMB's requirements under the Paperwork Reduction Act as well as GSA's own needs.

Senior Officials for Information Resources Management. In accordance with 44 U.S.C. 3506(b) and 5 CFR 1320.8, agencies are required to designate a senior official to carry out responsibilities under the Paperwork Reduction Act. The designation of the official is intended to assure clear accountability for setting policy for agency information resources management activities, provide for greater coordination among the agency's information activities, and ensure greater visibility of such activities within the agency. The responsibilities of the senior official for information resources management were identified in OMB Bulletin No. 81-21, which has expired. Those responsibilities are now established in this Circular.

International Information Policy. The Circular deals with the management of information resources held by the Federal government. While the creation, collection, processing, transmission, dissemination, use, storage, and disposition of information by the Federal government has international ramifications, Federal government information resources management policy is not the same as "U.S. information policy," which refers to U.S. national interests in the information field vis-a-vis the policies and interests of other nations. The Circular formally acknowledges this distinction and assigns responsibilities for international information policy only insofar as it relates to Federal government information resources management policy.

Timely Technology Procurement. Inherent in effective management of information technology is the ability of program managers to acquire technology in a timely manner. GSA is assigned the responsibility in Section 9 to develop criteria that will streamline procurement procedures and delegate procurement authority to agencies that comply with those procedures. All Federal agencies are directed in Section 9 to develop internal policies and procedures that further provide for timely acquisition of information technology.

Records Management. The Paperwork Reduction Act makes the management of Federal records an integral part of information resources management. While no new policies are embodied in this Circular, responsibilities have been assigned in order to ensure that agency records management programs are considered within the context of Federal information resources management.

Section 10. Oversight.

The broad scope of the Circular dictates a strategy of focusing oversight on a series of aspects of information resources management rather than on a single comprehensive reporting scheme. OMB intends to use existing mechanisms, such as the fiscal budget, information collection budget, and management reviews, to examine agency compliance with the Circular. For example, during 1984 the management reviews for the FY 1986 budget year concentrated on five cross-cutting information issues: overall information resources management strategy, telecommunications, software management, "electronic filing," and end user computing. OMB issued data call bulletins requesting information specific to these issues, targeted the issues for special attention during the management reviews, and requested individual agencies to submit management improvement plans on specific aspects of the issues. Pursuit of this kind of selective oversight strategy permits OMB and the agencies the flexibility to shift the focus of oversight as information issues and the technological environment change.

**ATTACHMENT 4**

**National Security Decision Directive 145 (NSDD-145):  
National Policy on Telecommunications  
and  
Automated Information Systems Security  
(September 17, 1984)**

THE WHITE HOUSE  
WASHINGTON  
September 17, 1984

*National Security  
Decision Directive 145  
(Unclassified Version)*

NATIONAL POLICY ON TELECOMMUNICATIONS  
AND AUTOMATED INFORMATION SYSTEMS SECURITY

Recent advances in microelectronics technology have stimulated an unprecedented growth in the supply of telecommunications and information processing services within the government and throughout the private sector. As new technologies have been applied, traditional distinctions between telecommunications and automated information systems have begun to disappear. Although this trend promises greatly improved efficiency and effectiveness, it also poses significant security challenges. Telecommunications and automated information processing systems are highly susceptible to interception, unauthorized electronic access, and related forms of technical exploitation, as well as other dimensions of the hostile intelligence threat. The technology to exploit these electronic systems is widespread and is used extensively by foreign nations and can be employed, as well, by terrorist groups and criminal elements. Government systems as well as those which process the private or proprietary information of US persons and businesses can become targets for foreign exploitation.

Within the government these systems process and communicate classified national security information and other sensitive information concerning the vital interests of the United States. Such information, even if unclassified in isolation, often can reveal highly classified and other sensitive information when taken in aggregate. The compromise of this information, especially to hostile intelligence services, does serious damage to the United States and its national security interests. A comprehensive and coordinated approach must be taken to protect the government's telecommunications and automated information systems against current and projected threats. This approach must include mechanisms for formulating policy, for overseeing systems security resources programs, and for coordinating and executing technical activities.

This Directive: Provides initial objectives, policies, and an organizational structure to guide the conduct of national activities directed toward safeguarding systems which process or communicate sensitive information from hostile exploitation; establishes a mechanism for policy development; and assigns

responsibilities for implementation. It is intended to assure full participation and cooperation among the various existing centers of technical expertise throughout the Executive Branch, to promote a coherent and coordinated defense against the hostile intelligence threat to these systems, and to foster an appropriate partnership between government and the private sector in attaining these goals. This Directive specifically recognizes the special requirements for protection of intelligence sources and methods. It is intended that the mechanisms established by this Directive will initially focus on those automated information systems which are connected to telecommunications transmission systems.

1. Objectives. Security is a vital element of the operational effectiveness of the national security activities of the government and of military combat readiness. Assuring the security of telecommunications and automated information systems which process and communicate classified national security information, and other sensitive government national security information, and offering assistance in the protection of certain private sector information are key national responsibilities. I, therefore, direct that the government's capabilities for securing telecommunications and automated information systems against technical exploitation threats be maintained or improved to provide for:

a. A reliable and continuing capability to assess threats and vulnerabilities, and to implement appropriate, effective countermeasures.

b. A superior technical base within the government to achieve this security, and support for a superior technical base within the private sector in areas which complement and enhance government capabilities.

c. A more effective application of government resources and encouragement of private sector security initiatives.

d. Support and enhancement of other policy objectives for national telecommunications and automated information systems.

2. Policies. In support of these objectives, the following policies are established:

a. Systems which generate, store, process, transfer or communicate classified information in electrical form shall be secured by such means as are necessary to prevent compromise or exploitation.

b. Systems handling other sensitive, but unclassified, government or government-derived information, the loss of which could adversely affect the national security interest,

shall be protected in proportion to the threat of exploitation and the associated potential damage to the national security.

c. The government shall encourage, advise, and, where appropriate, assist the private sector to: identify systems which handle sensitive non-government information, the loss of which could adversely affect the national security; determine the threat to, and vulnerability of, these systems; and formulate strategies and measures for providing protection in proportion to the threat of exploitation and the associated potential damage. Information and advice from the perspective of the private sector will be sought with respect to implementation of this policy. In cases where implementation of security measures to non-governmental systems would be in the national security interest, the private sector shall be encouraged, advised, and, where appropriate, assisted in undertaking the application of such measures.

d. Efforts and programs begun under PD-24 which support these policies shall be continued.

3. Implementation. This Directive establishes a senior level steering group; an interagency group at the operating level; an executive agent and a national manager to implement these objectives and policies.

4. Systems Security Steering Group.

a. A Systems Security Steering Group consisting of the Secretary of State, the Secretary of the Treasury, the Secretary of Defense, the Attorney General, the Director of the Office of Management and Budget, the Director of Central Intelligence, and chaired by the Assistant to the President for National Security Affairs is established. The Steering Group shall:

(1) Oversee this Directive and ensure its implementation. It shall provide guidance to the Executive Agent and through him to the National Manager with respect to the activities undertaken to implement this Directive.

(2) Monitor the activities of the operating level National Telecommunications and Information Systems Security Committee and provide guidance for its activities in accordance with the objectives and policies contained in this Directive.

(3) Review and evaluate the security status of those telecommunications and automated information systems that handle classified or sensitive government or government-derived information with respect to established objectives and priorities, and report findings and recommendations through the National Security Council to the President.

(4) Review consolidated resources program and budget proposals for telecommunications systems security, including the COMSEC Resources Program, for the US Government and provide recommendations to OMB for the normal budget review process.

(5) Review in aggregate the program and budget proposals for the security of automated information systems of the departments and agencies of the government.

(6) Review and approve matters referred to it by the Executive Agent in fulfilling the responsibilities outlined in paragraph 6. below.

(7) On matters pertaining to the protection of intelligence sources and methods be guided by the policies of the Director of Central Intelligence.

(8) Interact with the Steering Group on National Security Telecommunications to ensure that the objectives and policies of this Directive and NSDD-97, National Security Telecommunications Policy, are addressed in a coordinated manner.

(9) Recommend for Presidential approval additions or revisions to this Directive as national interests may require.

(10) Identify categories of sensitive non-government information, the loss of which could adversely affect the national security interest, and recommend steps to protect such information.

b. The National Manager for Telecommunications and Information Systems Security shall function as executive secretary to the Steering Group.

5. The National Telecommunications and Information Systems Security Committee.

a. The National Telecommunications and Information Systems Security Committee (NTISSC) is established to operate under the direction of the Steering Group to consider technical matters and develop operating policies as necessary to implement the provisions of this Directive. The Committee shall be chaired by the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) and shall be composed of a voting representative of each member of the Steering Group and of each of the following:

The Secretary of Commerce  
 The Secretary of Transportation  
 The Secretary of Energy

Chairman, Joint Chiefs of Staff  
 Administrator, General Services Administration  
 Director, Federal Bureau of Investigation  
 Director, Federal Emergency Management Agency  
 The Chief of Staff, United States Army  
 The Chief of Naval Operations  
 The Chief of Staff, United States Air Force  
 Commandant, United States Marine Corps  
 Director, Defense Intelligence Agency  
 Director, National Security Agency  
 Manager, National Communications System

b. The Committee shall:

- (1) Develop such specific operating policies, objectives, and priorities as may be required to implement this Directive.
- (2) Provide telecommunication and automated information systems security guidance to the departments and agencies of the government.
- (3) Submit annually to the Steering Group an evaluation of the status of national telecommunications and automated information systems security with respect to established objectives and priorities.
- (4) Identify systems which handle sensitive, non-government information, the loss and exploitation of which could adversely affect the national security interest, for the purpose of encouraging, advising and, where appropriate, assisting the private sector in applying security measures.
- (5) Approve the release of sensitive systems technical security material, information, and techniques to foreign governments or international organizations with the concurrence of the Director of Central Intelligence for those activities which he manages.
- (6) Establish and maintain a national system for promulgating the operating policies, directives, and guidance which may be issued pursuant to this Directive.
- (7) Establish permanent and temporary subcommittees as necessary to discharge its responsibilities.
- (8) Make recommendations to the Steering Group on Committee membership and establish criteria and procedures for permanent observers from other departments or agencies affected by specific matters under deliberation, who may attend meetings upon invitation of the Chairman.
- (9) Interact with the National Communications System Committee of Principals established by Executive Order

12472 to ensure the coordinated execution of assigned responsibilities.

c. The Committee shall have two subcommittees, one focusing on telecommunications security and one focusing on automated information systems security. The two subcommittees shall interact closely and any recommendations concerning implementation of protective measures shall combine and coordinate both areas where appropriate, while considering any differences in the level of maturity of the technologies to support such implementation. However, the level of maturity of one technology shall not impede implementation in other areas which are deemed feasible and important.

d. The Committee shall have a permanent secretariat composed of personnel of the National Security Agency and such other personnel from departments and agencies represented on the Committee as are requested by the Chairman. The National Security Agency shall provide facilities and support as required. Other departments and agencies shall provide facilities and support as requested by the Chairman.

6. The Executive Agent of the Government for Telecommunications and Information Systems Security. The Secretary of Defense is the Executive Agent of the Government for Communications Security under authority of Executive Order 12333. By authority of this Directive he shall serve an expanded role as Executive Agent of the Government for Telecommunications and Automated Information Systems Security and shall be responsible for implementing, under his signature, the policies developed by the NTISSC. In this capacity he shall act in accordance with policies and procedures established by the Steering Group and the NTISSC to:

a. Ensure the development, in conjunction with NTISSC member departments and agencies, of plans and programs to fulfill the objectives of this Directive, including the development of necessary security architectures.

b. Procure for and provide to departments and agencies of the government and, where appropriate, to private institutions (including government contractors) and foreign governments, technical security material, other technical assistance, and other related services of common concern, as required to accomplish the objectives of this Directive.

c. Approve and provide minimum security standards and doctrine, consistent with provisions of the Directive.

d. Conduct, approve, or endorse research and development of techniques and equipment for telecommunications and automated information systems security for national security information.

e. Operate, or coordinate the efforts of, government technical centers related to telecommunications and automated information systems security.

f. Review and assess for the Steering Group the proposed telecommunications systems security programs and budgets for the departments and agencies of the government for each fiscal year and recommend alternatives, where appropriate. The views of all affected departments and agencies shall be fully expressed to the Steering Group.

g. Review for the Steering Group the aggregated automated information systems security program and budget recommendations of the departments and agencies of the US Government for each fiscal year.

7. The National Manager for Telecommunications Security and Automated Information Systems Security. The Director, National Security Agency is designated the National Manager for Telecommunications and Automated Information Systems Security and is responsible to the Secretary of Defense as Executive Agent for carrying out the foregoing responsibilities. In fulfilling these responsibilities the National Manager shall have authority in the name of the Executive Agent to:

a. Examine government telecommunications systems and automated information systems and evaluate their vulnerability to hostile interception and exploitation. Any such activities, including those involving monitoring of official telecommunications, shall be conducted in strict compliance with law, Executive Orders and applicable Presidential Directives. No monitoring shall be performed without advising the heads of the agencies, departments, or services concerned.

b. Act as the government focal point for cryptography, telecommunications systems security, and automated information systems security.

c. Conduct, approve, or endorse research and development of techniques and equipment for telecommunications and automated information systems security for national security information.

d. Review and approve all standards, techniques, systems and equipments for telecommunications and automated information systems security.

e. Conduct foreign communications security liaison, including agreements with foreign governments and with international and private organizations for telecommunications and automated information systems security, except for those foreign intelligence relationships conducted for intelligence purposes by the Director of Central Intelligence. Agreements shall be coordinated with affected departments and agencies.

f. Operate such printing and fabrication facilities as may be required to perform critical functions related to the provision of cryptographic and other technical security material or services.

g. Assess the overall security posture and disseminate information on hostile threats to telecommunications and automated information systems security.

h. Operate a central technical center to evaluate and certify the security of telecommunications systems and automated information systems.

i. Prescribe the minimum standards, methods and procedures for protecting cryptographic and other sensitive technical security material, techniques, and information.

j. Review and assess annually the telecommunications systems security programs and budgets of the departments and agencies of the government, and recommend alternatives, where appropriate, for the Executive Agent and the Steering Group.

k. Review annually the aggregated automated information systems security program and budget recommendations of the departments and agencies of the US Government for the Executive Agent and the Steering Group.

l. Request from the heads of departments and agencies such information and technical support as may be needed to discharge the responsibilities assigned herein.

m. Enter into agreements for the procurement of technical security material and other equipment, and their provision to government agencies and, where appropriate, to private organizations, including government contractors, and foreign governments.

8. The Heads of Federal Departments and Agencies shall:

a. Be responsible for achieving and maintaining a secure posture for telecommunications and automated information systems within their departments or agencies.

b. Ensure that the policies, standards and doctrines issued pursuant to this Directive are implemented within their departments or agencies.

c. Provide to the Systems Security Steering Group, the NTISSC, Executive Agent, and the National Manager, as appropriate, such information as may be required to discharge responsibilities assigned herein, consistent with relevant law, Executive Order, and Presidential Directives.

9. Additional Responsibilities.

a. The Secretary of Commerce, through the Director, National Bureau of Standards, shall issue for public use such Federal Information Processing Standards for the security of information in automated information systems as the Steering Group may approve. The Manager, National Communications System, through the Administrator, General Services Administration, shall develop and issue for public use such Federal Telecommunications Standards for the security of information in telecommunications systems as the National Manager may approve. Such standards, while legally applicable only to Federal Departments and Agencies, shall be structured to facilitate their adoption as voluntary American National Standards as a means of encouraging their use by the private sector.

b. The Director, Office of Management and Budget, shall:

(1) Specify data to be provided during the annual budget review by the departments and agencies on programs and budgets relating to telecommunications systems security and automated information systems security of the departments and agencies of the government.

(2) Consolidate and provide such data to the National Manager via the Executive Agent.

(3) Review for consistency with this Directive, and amend as appropriate, OMB Circular A-71 (Transmittal Memorandum No. 1), OMB Circular A-76, as amended, and other OMB policies and regulations which may pertain to the subject matter herein.

10. Nothing in this Directive:

a. Alters the existing authorities of the Director of Central Intelligence, including his responsibility to act as Executive Agent of the Government for technical security countermeasures (TSCM).

b. Provides the NTISSC, the Executive Agent, or the National Manager authority to examine the facilities of other departments and agencies without approval of the head of such department or agency, nor to request or collect information concerning their operation for any purpose not provided for herein.

c. Amends or contravenes the provisions of existing law, Executive Orders, or Presidential Directives which pertain to the privacy aspects or financial management of automated information systems or to the administrative requirements for safeguarding such resources against fraud, abuse, and waste.

d. Is intended to establish additional review processes for the procurement of automated information processing systems.

11. For the purposes of this Directive, the following terms shall have the meanings indicated:

a. Telecommunications means the preparation, transmission, communication or related processing of information by electrical, electromagnetic, electromechanical, or electro-optical means.

b. Automated Information Systems means systems which create, prepare, or manipulate information in electronic form for purposes other than telecommunication, and includes computers, word processing systems, other electronic information handling systems, and associated equipment.

c. Telecommunications and Automated Information Systems Security means protection afforded to telecommunications and automated information systems, in order to prevent exploitation through interception, unauthorized electronic access, or related technical intelligence threats, and to ensure authenticity. Such protection results from the application of security measures (including cryptosecurity, transmission security, emission security, and computer security) to systems which generate, store, process, transfer, or communicate information of use to an adversary, and also includes the physical protection of sensitive technical security material and sensitive technical security information.

d. Technical security material means equipment, components, devices, and associated documentation or other media which pertain to cryptography, or to the securing of telecommunications and automated information systems.

12. The functions of the Interagency Group for Telecommunications Protection and the National Communications Security Committee (NCSC) as established under PD-24 are subsumed by the Systems Security Steering Group and the NTISSC, respectively. The policies established under the authority of the Interagency Group or the NCSC, which have not been superseded by this Directive, shall remain in effect until modified or rescinded by the Steering Group or the NTISSC, respectively.

13. Except for ongoing telecommunications protection activities mandated by and pursuant to PD/NSC-24, that Directive is hereby superseded and cancelled.

**ATTACHMENT 5**

**Telegrams:**

1985 State 378130: Processing of LOU Information  
1985 State 337721: LOU Processing  
1987 State 139964: Processing of LOU Information  
1987 State 132298: A.I.D. Information Systems  
Security Policy

122

UNCLASSIFIED  
Department of State

OUTGOING  
TELEGRAM

PAGE 01 STATE 378130  
ORIGIN AID-00

8842 077076 A103576

STATE 378130

8842 077076

ORIGIN OFFICE SIC-01  
INFO /001 A0

ATTACHMENT 5-1

INFO LOG-00 OCFE-00 EUR-00 SS-00 AF-00 IO-16 NEA-07  
ARA-00 LAP-00 DC-02 /025 A

DRAFTED BY: AID/IG/SEC:ATCLINE:UJS -  
APPROVED BY: AID/IG/SEC:ATCLINE  
AID/ES:GJOE AID/IG (INFO)  
AID/IRM:PPSPISNAK

-----153752 1206202 /30

R 120120Z DEC 85 ZEX  
FM SECSTATE WASHDC  
TO AID WORLDWIDE  
AMEMBASSY BEIRUT  
AMEMBASSY KAMPALA

UNCLAS STATE 378130

AIDAC

E.O. 12356: N/A  
TAGS:

SUBJECT: PROCESSING OF LOU INFORMATION

REF: (A) 1984 STATE 376373 (M) STATE 337721

1. REFERENCE (A) PROVIDED USAIDS WITH A SUMMARY OF AGENCY POLICY GUIDANCE ON CE FUNDED MISSION INFORMATION TECHNOLOGY PROGRAMS. INCLUDED IN THAT GUIDANCE IS A POLICY STATEMENT THAT MISSION DIRECTORS ARE RESPONSIBLE FOR THE TECHNICAL AND PHYSICAL SECURITY OF ALL HARDWARE AND SOFTWARE AT POST, AND FOR INSURING THAT NO CLASSIFIED MATERIAL, INCLUDING LIMITED OFFICIAL USE (LOU), IS PROCESSED ON THEIR POSTS' INFORMATION TECHNOLOGY SYSTEMS, INCLUDING WORD PROCESSORS, GISS, MICROCOMPUTERS, MINICOMPUTERS OR BY TELECOMMUNICATION.

2. IN ACCORDANCE WITH THE PROVISIONS OF REFERENCE (M), AGENCY RESTRICTIONS GOVERNING THE PROCESSING OF LOU MATERIAL ON UNCLASSIFIED AUTOMATED INFORMATION SYSTEMS OVERSEAS ARE HEREBY RESCINDED FOR THOSE USAIDS THAT ARE NOT LOCATED IN HIGH TECHNICAL-THREAT FOREIGN SERVICE POSTS. IN ORDER FOR THOSE USAIDS TO PROCESS LOU MATERIAL, THEY MUST FOLLOW THE CONDITIONS SPECIFIED IN REFERENCE (M).

3. MISSIONS IN HIGH TECHNICAL THREAT FOREIGN SERVICE POSTS MUST INSURE THAT LOU INFORMATION IS NOT PROCESSED AND/OR STORED ON AN UNCLASSIFIED SYSTEM. QUESTIONS CONCERNING HIGH TECHNICAL THREAT POSTS SHOULD BE ADDRESSED TO THE ASD, EPO, ISSO, OR IG/SEC/DIDS.

4. MISSIONS ARE REMINDED THAT CLASSIFIED MATERIAL MUST NOT BE PROCESSED ON UNCLASSIFIED AUTOMATED INFORMATION SYSTEMS. THERE WILL BE INSPECTIONS BY ASD, EPO, ISSO AND OR IG/SEC TO VERIFY THAT CLASSIFIED MATERIAL IS NOT BEING PROCESSED. FAILURE TO COMPLY WITH THIS REQUIREMENT COULD CONSTITUTE A SECURITY VIOLATION AND WOULD BE PROCESSED IN ACCORDANCE WITH THE UNIFORM SECURITY REGULATIONS.

5. IT MUST BE STRONGLY EMPHASIZED THAT REFTELS MUST BE REVIEWED AND COMPLIED WITH PRIOR TO IMPLEMENTATION OF THIS AUTHORITY TO PROCESS LOU IN NON HIGH TECHNICAL-THREAT LOCATIONS.

6. MINIMIZE CONSIDERED. WHITENEGD

DEC 12 8 37 AM '85

UNCLASSIFIED

123

AFFCTT WALTER  
ES STATE 337721

12/05/85 34-5537 PRINTER: F1

UNCLASSIFIED

UNCLASSIFIED

PAGE 01 STATE 337721

ORIGIN A-02

INFC	ICG-00	ADS-00	FUR-00	OPR-01	AF-00	MMC-01	IC-10
	NEA-07	ARA-00	SSO-00	SY-05	AMAD-01	EAP-00	AIT-02
	SIG-03	FSI-06	AS-00	CC-02	ISO-02	/251 R	

DRAFTED BY: ISS:EMARNEY:FM

APPROVED BY: ISS:IMCNUITY

A/SY:IFIELDS

A/CC/S:KKIDWELL

A/ISC:DMCUNT

A/OPR:JCCNDAYAN

A:IFOUCHARD

M/DSC:WFATON

AF/EX:TMCAHON

EAP/EX:EMCERISC

FUR/EX:JJACKSON

ARA/EX:MSSTONE

NEA/EX:RPEPPER

S/S-C:REYANHEUVEN

-----32243 021000Z /30

R 221020Z NOV 85 ZFX

FM SECSTATE WASHDC

TO ALL DIPLOMATIC AND CONSULAR POSTS

UNCLAS STATE 337721

Z.C. 12356:N/A

INFO: AADP

SUBJECT: ICU PROCESSING

1. REFERENCE STATE CABLE 307967, WHICH STATES THAT TEMPEST-APPROVED EQUIPMENT IS NO LONGER REQUIRED FOR ICU INFORMATION. POSTS ARE REMINDED THAT THIS POLICY ONLY CHANGES THE TEMPEST REQUIREMENTS FOR ICU. ALL OTHER CONTACTS OVER ICU INFORMATION (I.E., ACCESS, STORAGE, AND DESTRUCTION) HAVE NOT CHANGED. SEE 5 FAM 950 FOR APPLICABLE REGULATIONS ON ADMINISTRATIVELY CONTROLLED INFORMATION.

2. NATIONAL SECURITY DECISION DIRECTIVE 145 (NSDD 145)

UNCLASSIFIED

TMENGRHEHDC

PAGE 02 STATE 337721

CALLS FOR THE PROTECTION OF UNCLASSIFIED, SENSITIVE INFORMATION. NATIONAL POLICY DEFINING UNCLASSIFIED, SENSITIVE INFORMATION WILL SOON BE ISSUED FOR ALL FEDERAL DEPARTMENTS AND AGENCIES. ONCE THIS DEFINITION BECOMES NATIONAL POLICY, THE DEPARTMENT WILL NEED TO REVIEW THE DEFINITION OF ICU TO ENSURE CONFORMANCE WITH THIS POLICY.

3. IN THE MEANTIME, THE FOLLOWING CONDITIONS MUST BE MET IF ICU IS PROCESSED OR STORED ON UNCLASSIFIED AUTOMATED INFORMATION SYSTEMS.

4. ICU MAY HENCEFORTH BE PROCESSED ON NON-TEMPEST APPROVED INFORMATION SYSTEMS OPERATING IN THE 'SYSTEM HIGH' MODE, I.E., ACCESS TO A SYSTEM PROCESSING ICU INFORMATION IS RESTRICTED TO CLEARED AMERICAN CITIZENS AND THOSE FSNS WITH ICU CLEARANCES. THE SYSTEM HIGH MODE IS BEST SUITED FOR PERSONAL COMPUTERS AND SMALL CIS SYSTEMS

UNCLASSIFIED

UNCLASSIFIED

ATTACHMENT 5-3

AFFOCT WALTER  
85 STATE 337721

12/25/95 095527 PRINCE: FT

UNCLASSIFIED

(E.G., CIS 60 AND BELOW) WHERE ACCESS CAN BE LIMITED TO AMERICANS AND CLEARED FSNS.

5. ALL MAGNETIC MEDIA (HARD DISKS, DISKETTES, TAPES, PRINTER RIBBONS, ETC.) CONTAINING LOU INFORMATION MUST BE STORED IN APPROVED CONTAINERS AND OTHERWISE PROTECTED IN ACCORDANCE WITH 5 FAM 922. NO MAGNETIC MEDIA CONTAINING LOU INFORMATION WILL BE LEFT ON THE SYSTEM UNATTENDED FOR ANY REASON. THE 'SECURITY ERASE' FEATURE WILL BE USED TO DELETE LOU INFORMATION FROM SYSTEMS WITH NON-REMOVABLE DISKS (E.G., CIS 60 AND PCS WITH WINCHESTER DRIVES).

6. THE DEPARTMENT IS REVIEWING PROCEDURES FOR PROCESSING LOU ON LARGE, DISTRIBUTED SYSTEMS (E.G., WANG VS MINICOMPUTERS) THAT ARE OPERATIONALLY FEASIBLE, WHILE STILL ENSURING THE PROTECTION OF LOU DATA. UNTIL FURTHER

UNCLASSIFIED

UNCLASSIFIED  
PAGE 23 STATE 337721

GUIDANCE IS ISSUED, LOU MAY NOT BE PROCESSED OR STORED ON ANY SYSTEM UNLESS IT IS LIMITED TO AMERICANS AND CLEARED FSNS.

7. POSTS SHOULD NOT SEND SYSTEMS WITH NON-REMOVABLE DISKS APPROVED FOR THE PROCESSING OF LOU INFORMATION OUTSIDE OF THE EMBASSY FOR MAINTENANCE.

8. LOU INFORMATION WILL NOT BE PROCESSED AND/OR STORED ON AN UNCLASSIFIED SYSTEM AT ANY HIGH TECHNICAL THREAT FOREIGN SERVICE POST.

9. IT IS THE RESPONSIBILITY OF THE ISSC TO APPROVE THE USE OF AN UNCLASSIFIED SYSTEM FOR LOU PROCESSING AND ENSURE THAT ALL OF THE ABOVE CRITERIA ARE MET.

10. ANY QUESTIONS REGARDING THESE CONDITIONS FOR LOU PROCESSING ARE TO BE DIRECTED TO ISS. WHITEFAD

UNCLASSIFIED

UNCLASSIFIED

PAGE

21 PAGE 01 STATE 139964

7099 205714 A117031

02 ORIGIN AID-00

03 -----

04 ORIGIN OFFICE SEC-01

05 INFO AAAF-02 AFRA-03 AALA-01 AMAD-01 IG-01 SMO-02 OIFM-02

06 IGA-04 KAY-01 ES-01 PFLO-01 TELE-01 AAAF-01 /0200 PV

07 -----

08 INFO LOG-00 /000 R

09

10 DRAFTED BY: AID/IG/SEC/PSI:HM\*NCHESTER:MFR:3472D

11 APPROVED BY: AID/IG/SEC:CMFLANNIFY

12 AID/IG:PIPECKINGTON (INFO) IG/SEC/SEC/PSI:DVEYRD (INFO)

13 AID/ES:RCMEYER (INFO) AID/IRM:PPSPISPAK (PHONE)

14 -----260220 2806443 /38

15 R 080641Z MAY 87 ZEX

16 FM SECSTATE WASHDC

17 TO AID WORLDWIDE

19 UNCLAS STATE 139964

21 ADM AID

23 E.O. 12356: N/A

24 TAGS:

25 SUBJECT: PROCESSING OF LOU INFORMATION

27 (THIS IS A REPEAT OF A WIDE STATE 37813W, DATED 12/12/85.)

29 REF: (A) 1984 STATE 176373. (F) STATE 337721

31 1. REFERENCE (A) PROVIDED USAIDS WITH A SUMMARY OF

32 AGENCY POLICY GUIDANCE ON OE FUNDED MISSION INFORMATION

33 TECHNOLOGY PROGRAMS. INCLUDED IN THAT GUIDANCE IS A

34 POLICY STATEMENT THAT MISSION DIRECTORS ARE RESPONSIBLE

35 FOR THE TECHNICAL AND PHYSICAL SECURITY OF ALL HARDWARE

36 AND SOFTWARE AT POST, AND FOR INSURING THAT NO

37 CLASSIFIED MATERIAL, INCLUDING LIMITED OFFICIAL USE

38 (LOU), IS PROCESSED ON THEIR POSTS' INFORMATION

39 TECHNOLOGY SYSTEMS, INCLUDING WORD PROCESSORS, OIS,

40 MICROCOMPUTERS, MINICOMPUTERS OR BY TELECOMMUNICATION.

41

42 2. IN ACCORDANCE WITH THE PROVISIONS OF REFERENCE (B),

43 AGENCY RESTRICTIONS GOVERNING THE PROCESSING OF LOU

44 MATERIAL ON UNCLASSIFIED AUTOMATED INFORMATION SYSTEMS

45

46 OVERSEAS ARE HEREBY RESCINDED FOR THOSE USAIDS THAT ARE

01 NOT LOCATED IN HIGH TECHNICAL-THREAT FOREIGN SERVICE  
02 POSTS. IN ORDER FOR THOSE USAIS TO PROCESS LOU  
03 MATERIAL, THEY MUST FOLLOW THE CONDITIONS SPECIFIED IN  
04 REFERENCE (2).

05  
06 3. MISSIONS IN HIGH TECHNICAL THREAT FOREIGN SERVICE  
07 POSTS MUST INSURE THAT LOU INFORMATION IS NOT PROCESSED  
08 AND/OR STORED ON AN UNCLASSIFIED SYSTEM. QUESTIONS  
09 CONCERNING HIGH TECHNICAL THREAT POSTS SHOULD BE  
10 ADDRESSED TO THE RSO, CPO, ISSO, OR IG/SEC/PSI.

11  
12 4. MISSIONS ARE REMINDED THAT CLASSIFIED MATERIAL MUST  
13 NOT BE PROCESSED ON UNCLASSIFIED AUTOMATED INFORMATION  
14 SYSTEMS. THERE WILL BE INSPECTIONS BY RSO, CPO, ISSO  
15 AND OR IG/SEC TO VERIFY THAT CLASSIFIED MATERIAL IS NOT  
16 BEING PROCESSED. FAILURE TO COMPLY WITH THIS  
17 REQUIREMENT COULD CONSTITUTE A SECURITY VIOLATION AND  
18 WOULD BE PROCESSED IN ACCORDANCE WITH THE UNIFORM  
19 SECURITY REGULATIONS.

20  
21 5. IT MUST BE STRONGLY EMPHASIZED THAT REFTELS MUST BE  
22 REVIEWED AND COMPLIED WITH PRIOR TO IMPLEMENTATION OF  
23 THIS AUTHORITY TO PROCESS LOU IN NON HIGH  
24 TECHNICAL-THREAT LOCATIONS.

25  
26 5. MINIMIZE CONSIDERED. WHITEHEAD  
27

127