

PS 1237.11 INFORMATION SECURITY PROGRAMS



Change Notice

DIRECTIVE AFFECTED: 1237.11
CHANGE NOTICE NUMBER: CN 1237.11
DATE: 10/24/97

1. PURPOSE AND SCOPE. To characterize the significant changes in the Information Security Programs Program Statement. The scope of this policy has been expanded to include both electronic and paper-based information, as well as computer and telecommunications systems. The current version of this Program Statement is entitled, "Computer Security." This revised policy provides more flexibility and options, fewer restrictions and prompts executive staff support concerning the management of Information Security at the local level.

2. SUMMARY OF CHANGES.

a. Information Security Officer. The Computer Systems Security Officer (CSSO) has been replaced with an elevated Information Security Officer (ISO) with broader responsibilities as collateral duties. This staff member will work with all institution departments and disciplines to more effectively protect information resources. The ISO will also collaborate with the local Public Information Officer (PIO), to advise staff and provide guidance in the handling and protection of sensitive information by any process or form.

The ISO may now delegate specific responsibilities to assistant ISOs.

b. Chief Executive Officer. The Chief Executive Officer (CEO) is no longer required to submit security officer appointments when a filled Computer Services Manager position exists.

c. Public Information Officer. Additional, although minor, responsibilities have been given to the local PIO to assist in

defining sensitive information. This enables the ISO to have the additional support and guidance needed when dealing with sensitive information.

d. **Computer Rooms**. There is greater clarification concerning controlled access to local Computer Rooms. Other than as the authorizing official, the CEO's name is not required to appear on the Entry Authority Listing (EAL).

e. **Office of Information Systems**. The Office of Information Systems (OIS) and Computer Services Managers are now exempted from previous restrictions that could impede software testing and evaluation.

f. **Department Heads**. Department heads are now held responsible for the security of information within their work areas.

g. **LAN Administrator Training**. All LAN administrators are now required to receive some level of training. The discipline responsible will determine the acceptable training level to effectively manage a particular network.

h. **Information Security Committee Membership**. Formerly the Computer Security Committee, this committee has been modified to a more manageable size and the Warden is provided with more discretionary authority for meeting schedules, membership and attendance excusals. An Associate Warden of the Warden's choosing will chair the committee and the policy adds the Attorney/Paralegal, PIO, Case Management Coordinator (CMC), and National Crime Information Center (NCIC) Coordinator to the membership.

i. **Sensitive Information Defined**. The term "sensitive information" is better defined to include specific examples of information that would be considered sensitive.

j. **Computer System Labeling**. The physical labeling requirements for computer systems has been reduced. Now, for the most part, only the "INMATE ACCESS" label will be placed on workstation equipment. "STAFF ONLY" labels are no longer

required and Department of Justice (DOJ) label will only be required for locations processing National Security Information (NSI). A waiver was requested from and granted by DOJ.

k. **Sensitive Media Purging And Disposition.** More cost-effective alternatives are authorized for the removal of sensitive data from fixed disks and removable media and destruction of media itself.

l. **Software Standards.** Only minimum security standards for software are prescribed, thus allowing OIS to set any standards necessary.

m. **UNICOR/Inmate Access.** A simple systems security alternative is authorized for UNICOR and other inmate-access systems; the use of Windows NT as an operating system. This will cause an almost immediate reduction in the use of historically difficult security software, as well as other conflicts and compliance problems. Establishes Windows NT as the preferred systems security for inmate-access systems.

UNICOR now has greater latitude in the area of information security compliance in order to increase productivity, raise competitiveness in the business market and increase profits. They will face fewer delays involving inmate screenings, accept greater risks unrelated to the Bureau, use the most beneficial technology and comply with Bureau policy without undue restriction.

n. **Physician Background Investigation Exemption.** A partial exemption has been granted for visiting or consulting physicians from the background investigation requirement. As long as inappropriate system areas are not accessed without suitable supervision, physicians may access inmate electronic or hard copy medical records in order to diagnose and treat inmate patients.

o. **Inmate Computer-Use Assignments And Management.** The use of Case Management Activity (CMA) assignments in SENTRY for computer use has been discontinued. Since these assignments are not transferred to another institution, only a local database will be required. Derogatory information (computer crime only) will be placed in the inmate's central file and a local database for further reference at current or future institutions.

The policy no longer mandates the assignment of an inmate to "Computer No" for disciplinary action taken concerning computers. Research of other Bureau policies revealed the existence of

provisions specifically addressing disciplinary measures for misuse of equipment and failing to obey instructions, etc.

Institutions now have greater latitude in the management of inmates accessing computer systems. Technology and the computer era continue to advance and the general population's knowledge of computers no longer make it practical to overly restrict inmate usage from the Central Office level. Most decisions concerning this area can be made without Bureau policy mandating inappropriate and quickly outdated procedures.

p. **Incoming Publications for Inmates.** Inmates are now only prohibited from receiving publications that pertain to the computer underground or hacker magazines and periodicals.

q. **Software Accountability.** Using a particular database for software accountability is no longer mandated. This will enable the field to comply with federal standards and choose the most practical method for them and at the same time, keep up with the OIS supported technology and eliminate duplicate record keeping systems.

r. **Inmate Computer Course Approval.** Approvals for inmate computer courses will now be accomplished at region level instead of the Central Office.

s. **Anti-Virus Management.** The management of anti-virus protection for workstations must now be performed at the server level. This is a more effective and economical means of safeguarding the Bureau from virus infections.

t. **Annual Training.** The Information Security segment at Annual Refresher Training has been expanded by an additional 15 minutes (from 30 to 45 minutes) to more adequately address the definition and protection of sensitive information. This change is based upon need and also responds to recorded findings during the last Central Office Program Review, DOJ Systems Security Evaluation and miscellaneous Compliance and Program Reviews.

u. **Documented Procedures**. Written procedures are now mandatory as a remedy for numerous Program Review deficiencies and management difficulties. The institutional supplement has returned as one of the options afforded the ISO.

v. **LAN System Backups**. Accelerated storage safeguards, previously delayed until the year 2000 for all system backups, must be established sooner for LANs.

3. **ACTION**. File this Change Notice in front of the Information Security Programs Program Statement.

/s/
Kathleen M. Hawk
Director



Program Statement

OPI: IPD
NUMBER: 1237.11
DATE: 10/24/97
SUBJECT: Information Security
Programs

1. PURPOSE AND SCOPE. To require that each Bureau office and institution (including Federal Prison Industries and the National Institute of Corrections) establish and implement information security programs that provide cost-effective safeguards and controls for all computers and telecommunications equipment and for all sensitive information, computer systems, terminals, software, and data and voice communications systems. Telecommunications systems are interfaced with or operated by computers and are therefore governed by security requirements for computer systems. Each security program must include at least the minimum administrative, physical, and personnel safeguards and controls prescribed in this Program Statement.

To ensure compliance with copyright laws and license agreements, each office and institution is required to use a standard software accountability system, which includes a complete and accurate inventory of software, procedures for regular reviews, and effective management controls.

This program implements Office of Management and Budget (OMB) Circular No. A-130, Appendix III, which requires that Executive Branch departments implement computer security programs.

Not included in this program statement are the processing and handling of CLASSIFIED or national security information (NSI), which must be approved by the Bureau's Information Security

Programs Section (ISPS), in compliance with Department of Justice 28 CFR Part 17, National Security Information Program; Revision, Final Rule.

Computer systems, particularly remote electronic communications, present unique security problems because of the amount of data handled and the difficulty of detecting and preventing security breaches. Public concerns have been raised about the criminal and privacy risks associated with automated processing of personal, proprietary, and other sensitive data.

Information stored in or processed by a computer system requires a level of protection commensurate with its sensitivity or monetary value.

The Privacy Act of 1974 requires that disclosure of specified information be limited to authorized persons and agencies. All sensitive information must be protected while being processed, stored, transmitted, or otherwise handled.

2. PROGRAM OBJECTIVES. The expected results of this program are:

a. The security of information, computers, terminals, telecommunications, and data communications systems will be maintained.

b. Computer software installed on any Bureau computer system will be legally purchased and licensed and used in compliance with the licensing agreement of the software vendor.

c. Staff who use or supervise the use of Bureau computer systems will be informed about their responsibilities with regard to information and computer security and trained to meet those responsibilities.

3. DIRECTIVES AFFECTED

a. Directive Rescinded

PS 1237.09 Computer Security (8/1/95)

b. Directives Referenced

PS 1232.04	Personal Computers (9/29/94)
PS 1237.10	Personal Computers, Network Standards Manual (6/18/97)
PS 1351.04	Release of Information (12/5/96)
PS 3000.02	Human Resource Management Manual (11/1/93)
PS 3420.08	Standards of Employee Conduct (3/7/96)
PS 3906.16	Employee Development Manual (3/21/97)
PS 5266.07	Incoming Publications (11/1/96)
PS 5580.05	Personal Property, Inmate (9/30/96)

c. Other References

101 U.S.C. 1724	Computer Security Act of 1987
E.O. 10450	Security Requirements for Government Employment
DOJ Order 2620.7	Limited Official Use
DOJ Order 2610.2A	Employment Security Regulations
DOJ Order 2640.2C	Telecommunications and Automated Information Systems Security
OMB Circular A-130	Appendix III, Management of Federal Information Resources
NIST PUB 500-172	Special Publication on Computer Security Training Guidelines
OMB Bulletin 90-08	Guidance for Preparation of Security Plans for Federal Computer Systems that Contain Sensitive Information
FIPS PUB 87	Guidelines for ADP Contingency Planning
FIPS PUB 112	Password Usage
28 CFR Part 17	Classified National Security Information and Access to Classified Information

4. STANDARDS REFERENCED

a. American Correctional Association Standards for Adult Correctional Boot Camp Programs: 1-ABC-1F-01, 1-ABC-1F-03, 1-ABC-1F-04.

b. American Correctional Association 3rd Edition Standards for Adult Correctional Institutions: 3-4097, 3-4098, 3-4103.

c. American Correctional Association 3rd Edition Standards for Adult Local Detention Facilities: 3-ALDF-1F-01, 3-ALDF-1F-02.

d. American Correctional Association 2nd Edition Standards for Administration of Correctional Agencies: 2-CO-1F-02, 2-CO-1F-06.

5. ACTION

a. Each Assistant Director, Regional Director, Warden, and Directors of training facilities shall appoint an Information Security Officer (ISO) to manage and coordinate the overall Information Security Program. In addition, these officials shall notify the Bureau's Security Programs Manager of the name of the appointed ISO, except where noted.

In addition, each Warden shall establish an Information Security Committee chaired by an Associate Warden, as detailed in Sections 1 and 2.

b. Community Corrections Management Offices or other geographically separated offices shall be included in the Information Security Program in the region to which they are assigned. Any office assigned to, but geographically separated from the Central Office, shall have an ISO appointed.

c. All staff who handle sensitive information by any means, access computers or telecommunications systems in the performance of their duties, or supervise the use of such systems shall follow the procedures and meet the requirements of this Program Statement and referenced directives.

d. Documentation required by this Program Statement shall be retained on file for at least two years; one year active and one year inactive.

/s/

Kathleen M. Hawk
Director

Table of Contents

1. RESPONSIBILITIES

- a. Security Program Manager (SPM)
- b. Computer Security Program Manager (CSPM)
- c. UNICOR Information Security Officer
- d. Chief Executive Officer (CEO)
- e. Public Information Officer (PIO)
- f. Information Security Officer (ISO)
- g. Assistant Information Security Officer (AISO)
- h. Computer System Users
- i. Computer System Application Developers
- j. LAN and Other Computer Systems Administrators
- k. Accrediting Authority (AA)
- l. Employee Development Managers

2. INFORMATION SECURITY COMMITTEE

- a. Duties
- b. Membership
- c. Meetings

3. REPORTING INFORMATION AND COMPUTER SECURITY VIOLATIONS AND VIRUS INCIDENTS

4. INFORMATION PROTECTION

- a. Information Sensitivity
- b. Systems Design
- c. Labeling of Computers and Terminals
- d. Protection of Sensitive Information on Electronic Media
 - (1) Labeling of Removable Media
 - (2) Securing Removable Media
 - (3) Fixed Disks
 - (4) Removal of Sensitive Data From Media
 - (5) Backups of Storage Media
 - (6) Data Recovery
 - (7) Control of Output
- e. Processing Sensitive Data Away From the Work Site
 - (1) Delegation
 - (2) Removal of Sensitive Information From the Work Site
 - (3) Processing of Sensitive Information on Government-Owned Equipment Away From the Regular Work Site

(4) Use of Non-Government-Owned Equipment to Perform Government Business

5. PHYSICAL SECURITY

- a. Computer Room
- b. Computer Room Security

6. SYSTEM ACCESS CONTROLS

- a. Access to Sensitive Data
 - (1) System User Identification
 - (2) Remote Terminals and Workstations
- b. Movement of Personnel
 - (1) Transfer of Staff
 - (2) Departing Employees
 - ◆ Notification of Departure
 - ◆ Separations
 - ◆ Backup
 - ◆ Disposition
 - ◆ Reassignment of Resources
 - (3) Temporary Deactivation of User Accounts
- c. Access to DOJ Data Center
 - (1) TOP SECRET and SENTRY Extended Security System (ESS)
 - (2) Issuing Authority
 - (3) Creating Personal User ID's
- d. Password Integrity
- e. Security of Computer Communication Links
- f. Remote Access Rules For Bureau Computer Systems
 - (1) Knowledge Requirement
 - (2) Data Transmittal Between Computers
 - ◆ Attended Operation
 - ◆ Unattended Operation
 - (3) Remote Control
- g. PC Networks

- h. Personal Computers
 - (1) Power-on Password
 - (2) Keyboard Inactivity
 - (3) Exception

7. PERSONNEL SECURITY

- a. Computer System Positions
- b. User Access Clearance Requirement
- c. Computer Room Access
- d. Access Authorization
- e. Non-BOP Personnel

8. ACCREDITATION

- a. Requirement
- b. System Security Plans
- c. Risk Analysis
- d. Contingency Plans
- e. Certification
- f. Accrediting
- g. Documentation

9. INMATE USE OF COMPUTERS

- a. Computer Use Categories (CUC)
- b. Physical Controls
- c. Application Development
- d. Data Entry
- e. Document Scanners
- f. Utility Software
- g. Computer Repair
- h. Task-Specific Configuration
- i. PC Security Software
- j. Staff Access Only vs. Staff and Inmate Access PCs
- k. Control of Media
 - (1) Disk Control
 - (2) Hard Drive Requirement
 - (3) Printouts
- l. Occupational Training and Education Programs
- m. Electric/Electronic Typewriters/Word Processors

- n. Electronic Calculators, Dictionaries, Etc.
- o. Prohibited Publications

10. SOFTWARE

- a. Software Licensing
- b. Software Development
- c. Software Distribution
- d. Software Accountability
 - (1) PC Users
 - (2) Warehouse/Receiving Staff
 - (3) ISO/AISO
 - (4) Documentation and Records
 - (5) Software Transfer
 - (6) Outdated Software--Distribution
 - (7) Audits

11. COMPUTER VIRUSES

- a. Virus Scanning
- b. Suspected Viruses
- c. Virus Containment and Removal
- d. Scanning Prior to Processing

12. INFORMATION AND COMPUTER TRAINING FOR STAFF

- a. Inmate Supervision
- b. LAN Administrators
- c. Security Training
 - (1) Instructors
 - (2) Initial Training
 - (3) Lesson Plans
 - (4) Initial Training Content
 - (5) Local Training Procedures
 - (6) Continuing Procedures
 - (7) Annual Training
- d. Training Record

GLOSSARY

1. RESPONSIBILITIES

a. Security Programs Manager (SPM)

(1) Coordinate all non-custody security programs with the Department of Justice.

(2) Report security violations, including virus infections, to the Department Security Officer (DSO) in writing.

(3) Assume the authority of Chief, Information Security Programs Section (ISPS), and direct the duties of the Computer Security Program Manager (CSPM).

b. Computer Security Program Manager (CSPM)

(1) Manage and direct the national Bureau Information Security Programs. Report program status to the SPM.

(2) Maintain a list of Information Security Officers (ISOs).

(3) Coordinate and monitor performance of Bureau computer risk analyses, system security plans, contingency plans, and compliance reviews.

(4) Provide a list of Central Office-managed or -governed systems designated as sensitive and/or operationally critical.

c. UNICOR Information Security Officer

(1) Ensure that UNICOR information, computer systems, and operations comply with provisions of this Program Statement.

(2) Monitor reports of security violations and virus incidents involving UNICOR systems.

(3) Immediately report UNICOR security violations and virus incidents to the CSPM.

d. Chief Executive Officer (CEO)

(1) Ensure the Information Security Program at each Bureau location is carried out within the guidelines of this Program Statement.

(2) At institutions, determine which systems are operationally critical and provide written designation as such.

(3) Designate an ISO and submit his/her name to the SPM in writing. Submit a new notice whenever a designation changes. By virtue of this policy, when a filled Computer Services Manager (CSM) position exists, the CSM is automatically designated the ISO. No written notification is required.

(4) Serve as Accrediting Authority (AA) for sensitive computer systems for which he/she has oversight.

(5) Accept and sign the results of contingency plan testing and authorize necessary corrective actions to improve the planning process.

(6) Approve local procedures for the secure storage and handling of hard copy sensitive documentation and printouts used for Bureau business.

e. Public Information Officer (PIO)

(1) Provide advice and suggested guidance to the ISO to ensure the established safeguards for sensitive information are adequate.

(2) Coordinate written procedures and other actions required by this Program Statement.

f. Information Security Officer (ISO)

(1) Establish and direct the local information security program, which encompasses the computer and telecommunications security programs. Ensure the implementation of security measures is commensurate with the sensitivity of information maintained at the site. Develop, and submit for the Warden's approval, written procedures for safeguarding sensitive information. These procedures may take the form of an Institution Supplement, addenda to existing system security plans, or memoranda.

(2) Assist employees with information security matters, including safeguarding and marking sensitive information.

(3) Report security violations and virus infections to the CEO and the Information Security Programs Section (ISPS). Minor violations (determined by the CEO) do not require a report to ISPS; a description and disposition of the incident shall be

documented and maintained locally. Using the proper format or other means prescribed by ISPS and providing all required information concerning the incident, the following violations shall be reported to ISPS:

- ◆ Unauthorized software.
- ◆ Unlicensed software.
- ◆ Introduction of malicious code.
- ◆ Unauthorized telecommunications and theft of services.
- ◆ Misuse of access IDs and passwords.
- ◆ Unauthorized access to DOJ/BOP computers or networks or access exceeding what is authorized.
- ◆ Failure to properly label storage media.
- ◆ Improper equipment and media disposal.
- ◆ Improper maintenance.
- ◆ Improper physical control.
- ◆ Theft or destruction of computer resources.
- ◆ Improper equipment disposal.
- ◆ Inmate use of staff computers.

Other violations are not reportable, but local documentation shall be completed and maintained to show what action was taken and that the condition was corrected.

(4) Provide advice to AISOs concerning computer system media containing sensitive information.

(5) Request guidance from the SPM on matters concerning the handling and storage of National Security Information (NSI).

(6) Recommend the designation of Assistant Information Security Officers (AISOs), as needed, to adequately implement and maintain the Information Security Program. All LAN administrators shall be at least AISOs. Regional ISOs shall ensure the appointment of an AISO from each Community Corrections Management (CCM) Office and any other offices administered by the CCM.

(7) Direct and determine the duties of the AISO.

(8) Provide guidance to system administrators in the development of system security plans and contingency plans, as described in this Program Statement, which protect computer resources and ensure that essential functions continue if computer support is interrupted.

(9) Ensure security is adequately addressed, in accordance with this policy, for areas with automated or computerized

telecommunications equipment such as PBXs, telephone switches, communications servers, modems, teletype terminals, and dial-up terminals or workstations.

g. Assistant Information Security Officer (AISO)

(1) Perform the duties of the ISO (as stated above) for a specific department, office, location, computer system, or systems. At least the following individuals will be designated as AISOs: all LAN administrators, PBX administrator, UNICOR computer specialist/system administrator, SIS, and communications technician/specialist.

(2) Serve as Acting ISO, if so designated.

(3) Report to the ISO any changes or incidents involving computer systems that may affect information security.

Note: The AISO for UNICOR shall report security violations and virus incidents to the UNICOR ISO and institution ISO, in addition to any other required reporting.

h. Computer System Users

(1) Protect sensitive information, in any form, from loss or unauthorized disclosure. Use only assigned IDs and passwords to access systems and data. Safeguard all forms of sensitive information assigned or left in their care.

(2) Physically situate computer systems safely and securely to avoid accidents, injuries, or unauthorized viewing of displayed data. Take reasonable precautions to avoid loss of or damage to Government property and information. Be knowledgeable of and adhere to local procedures for the secure storage and handling of sensitive documentation and printouts.

(3) Ensure that software installed on an assigned workstation is legally licensed. Where multiple users access the same computer, the supervisor having management oversight of the computer shall designate one user to be responsible for legitimate software use.

(4) Become familiar with information security requirements for computer systems, including Bureau policy and appropriate systems security and contingency plans.

(5) When circumstances warrant, grant access to files under their care to other staff when directed to do so by the Assistant Director/Deputy, Regional Director/Deputy, Warden, or Associate Warden. The action shall be in writing.

(6) Be responsible for security of individual and shared office space containing computers, sensitive printouts, and electronic storage devices/media. All persons entering Bureau offices shall be known to assigned staff in their particular office space, unless escorted by authorized staff members.

(7) Ensure, when leaving a PC, system, terminal, etc., unattended, all systems are logged off or a security feature is engaged to prevent unauthorized use. Communications links shall be terminated when no longer needed.

i. Computer System Application Developers

(1) Include appropriate information safeguards and security in an application system's life cycle design.

(2) Perform a risk analysis of their application systems.

j. LAN and Other Computer Systems Administrators

(1) Every three years, complete a system security plan, risk analysis, contingency plan, certification, and accreditation for each system for which they are responsible. Contingency plans shall be continually updated as needed.

(2) Ensure that all software installed on hard drives under their control is licensed.

(3) Serve as at least an AISO, if not previously appointed as a ISO.

(4) LAN administrators shall receive training for each system they administer. Where LANs are connected to BOPNet, Office of Information Systems (OIS) shall establish the training minimums. Training standards for non-BOPNet-connected systems shall be set by the Central Office division having oversight. Official training records shall reflect the completion of suitable training achieved by Bureau-determined or software manufacturer-determined instruction. Minimum training standards shall be established by the applicable discipline.

k. Accrediting Authority (AA)

(1) The designated Senior Accrediting Authority (SAA) for the Bureau is the Assistant Director, Information, Policy, and Public Affairs Division. Only the SAA shall accredit systems processing National Security Information (NSI).

(2) Chief Executive Officers are designated AAs for sensitive computer systems under their purview. The accreditation process shall be facilitated by the designated ISO.

(3) AAs certify, based upon the ISO's recommendation, that system documentation and safeguards are within the bounds of acceptable risk. Significant changes affecting (enhancing or degrading) the system's security or operation made during its life cycle shall be formally documented and coordinated with the AA. Changes of lesser importance, not affecting the level of security protection, may be noted on or attached to system security documentation and later incorporated upon the first required review.

1. Employee Development Managers. Coordinate and document Information Security and other related training.

2. INFORMATION SECURITY COMMITTEE

a. Duties. Each CEO shall establish an Information Security Committee for the institution to:

(1) Develop, implement, and maintain information security procedures, institution supplements (where applicable), computer system security plans and addenda, contingency plans, system certifications, and accreditation records.

(2) Monitor adherence to copyright laws; annually test contingency plans; review reports of computer reviews, system evaluations, virus incidents, and security violations; and semiannually report to the CEO on the facility's information security status.

b. Membership. The CEO shall appoint an Associate Warden to chair the committee. Membership shall include, but is not limited to, the Public Information Officer (PIO), ISO, SIS, Communications Technician/Specialist, Attorney/Paralegal, Case Management Coordinator, NCIC Coordinator, and all LAN administrators.

c. Meetings. The committee shall meet at least quarterly and whenever significant security issues arise. Only the CEO or designee may authorize the cancellation of a regular meeting or excuse a required member's absence. The excused member shall ensure that a representative is sent in his or her place during non-emergency situations. A record of attendees, subjects discussed, and decisions reached shall be on file with the committee chair. Copies shall be distributed to each member.

3. REPORTING INFORMATION AND COMPUTER SECURITY VIOLATIONS AND VIRUS INCIDENTS

Security violations and suspected or actual virus infections shall be reported in writing. When a violation or virus infection occurs, the ISO shall, within 24 hours of receiving notice of such infection, notify ISPS via GroupWise E-mail to "COMPUTER SECURITY" (copy to CEO and Regional ISO), in the approved format, detailing facts and events concerning the violation or virus.

It is the discovering ISO's responsibility to notify other locations and ISOs that may become virus recipients or who may have originated the virus. The ISO shall forward a copy of these notifications to ISPS, unless included in the required report.

4. INFORMATION PROTECTION

a. Information Sensitivity. Sensitive information must be protected against release to or interception by unauthorized individuals. It requires protection due to the risk of loss or harm that could result from accidental or intentional disclosure, modification, or destruction. The degree of sensitivity and protection depends upon factors such as the quantity, age, and value of the data to unauthorized personnel. Information sensitivity shall be determined in accordance with this Program Statement or referenced directives, subject matter policies, and similar guidance; and by the discipline or department responsible for using the information. This action shall be coordinated with the PIO and ISO. When a clear decision cannot be made, a written request shall be submitted for resolution to ISPS. Sensitive information shall include:

(1) Information subject to the Privacy Act of 1974; i.e., Social Security numbers, home addresses and phone numbers, marital status, race, religion, staff performance evaluations, and other personal information recorded in the Official Personnel File of staff or files of inmates.

(2) Information that could be manipulated for personal profit or to hide the unauthorized use of money, equipment, or privileges.

(3) Investigative data.

(4) Proprietary data; i.e., industry programming code or encryption algorithms, information compiled or developed for in-house use only, selected budgetary data, procurement bids, etc.

(5) Information to which access is restricted to authorized personnel by law or directive.

(6) Information critical to the Bureau's or institution's operation and mission; i.e., WitSec information, lock and key data, gang or organized crime intelligence, and institution emergency plans.

(7) Information subject to the Tax Reform Act of 1976; i.e., personal income tax returns or information extracted from them.

(8) Grand jury information subject to the Federal Rules of Criminal Procedure, Rule 6(e), Grand Jury Secrecy of Proceedings and Disclosure.

(9) Information used by automated decision-making systems that have a high potential for financial loss.

(10) Information exempt from the Freedom of Information Act (FOIA), 5 U.S.C. 552a.

(11) Software or hardware manuals that provide information on system security features.

(12) Information specifically designated "Limited Official Use (LOU)."

(13) Other information which, if released, might cause harm to any person, adversely affect a Federal program, or whose release is prohibited by law or regulation.

In summary: Any information that is not releasable to the general public or to other persons who do not have a genuine need to know. If the disclosure of the information is restricted or subject to PA/FOIA screening, it is considered sensitive.

b. Systems Design. The data flow for sensitive systems shall be analyzed to determine where controls may be needed to protect against data loss, destruction, or modification and to ensure that such events will be detected. Such controls shall be implemented by the system application developer for all new systems and existing systems where economically feasible.

c. Labeling of Computers and Terminals. All PCs, workstations, and terminals shall be labeled: "THIS MACHINE IS NOT AUTHORIZED FOR CLASSIFIED PROCESSING" in a clearly visible location. Locally produced labels are recommended.

An exception is permitted for Bureau locations that meet the following qualification where NSI processing is not authorized:

Instead of affixing a physical label to the equipment, configure each system to make the same statement appear to the user (replacing "MACHINE with SYSTEM") prior to accessing any applications. For personal computers without network connection, the booting sequence would pause and display the wording directly beneath the required warning banner referred to in Section 6, paragraph g.(1) (if applicable), or at any point prior to accessing directories or files. For network workstations booting to the network ID and password prompt, this statement would be displayed after the warning banner (see paragraph 6.g. for an example).

d. Protection of Sensitive Information on Electronic Media. Removable media shall be categorized based on their content and protected as all other information and files are protected.

(1) Labeling of Removable Media. All removable media containing sensitive information shall be clearly labeled or marked with the contents and "SENSITIVE-LIMITED OFFICIAL USE" or "LIMITED OFFICIAL USE." The abbreviation/acronym "SENS-LOU" or acronym "LOU" alone are both permissible.

(2) Securing Removable Media. When unattended, removable media containing sensitive data shall be stored in a locked desk drawer, locked file cabinet, locked office, safe, etc., or in an area with controls adequate to prevent unauthorized access, disclosure, damage, modification, or destruction. Removable media must be protected from inadvertent erasure.

(3) Fixed Disks. PCs with sensitive data stored on their fixed disks shall be maintained in a secure area or otherwise protected from access by unauthorized persons.

(4) Removal of Sensitive Data From Media. All fixed or removable media shall be destroyed or shall have sensitive data permanently removed prior to disposal, declaration as surplus, or transfer to a person not authorized to access the information. Overwriting of data using utility programs (such as Norton WIPEINFO with the "/G" switch, or PC TOOLS) that meet the U.S. Department of Defense Standard (DOD 5220.22M) and the DOS format "/U" switch version 6.20 and above may be used to remove sensitive information.

Floppy disks may be destroyed by removing the interior disk and running it through a mechanical shredder (or intact through a

heavy-duty shredder) or by cutting it into small pieces and discarding with non-recyclable waste materials. Printouts may be destroyed in the same fashion. Floppy disks do not require degaussing or overwriting prior to physical destruction.

Fixed disks, or other media that cannot be shredded or overwritten, shall be sent to the Office of Information Systems (OIS), PC Support, for degaussing. Such a shipment shall be by certified mail or other Government-approved delivery service, with a return receipt required. Enclose disposition instructions; i.e., the address to which the degaussed media should be forwarded. Local degaussing is authorized using available bulk erasers, provided each eraser is tested and the procedures are approved by ISPS. Identical procedures shall be followed for all future degaussing and documented. Other local degaussing or methods of data destruction require written approval from ISPS.

Compact disks may be crushed or broken by methods that will safeguard against personal injury. Hard copies (paper) may be shredded or torn into small pieces and discarded with other waste materials or recycled.

The software used to overwrite sensitive data shall be protected at the same level as the information contained on the media, due to the remote chance that data may be transferred. Keep in mind that, with the advanced technology available today, information can be recovered from destroyed media in varying conditions. A reasonable effort shall be made to destroy and prevent sensitive information from reaching unauthorized persons. As long as a genuine attempt is applied to prevent reconstruction or recovery by normal methods, it is deemed acceptable.

(5) Backups of Storage Media. Backup copies of critical data shall always be created, updated regularly, and securely stored in an offsite location (outside the institution's secure perimeter) or in a fire-rated container designed for electronic media. These containers are designed to maintain their internal temperature-humidity ranges (RH) below 65.5 degrees Centigrade (150 degrees Fahrenheit) and 85% RH for periods up to four hours, two hours, or one hour. Refer to OIS for specific guidance concerning critical backups and frequency.

Existing fire-rated containers, not necessarily designed for the protection of electronic media, may be used until January 1, 2000, with the exception of LAN backups. Within six months of the publication of this policy, all LAN backups shall be stored

in electronic media-specific fire-rated containers, if not stored offsite.

Critical backups shall be performed frequently enough to prevent serious interference with operations due to data loss. The CEO, CEO-designee or department head shall determine what data is operationally critical. Users are responsible for backing up their data on a PC's hard drive. The LAN Administrator is responsible for the file server. Backup copies of sensitive data shall be labeled and protected in the same manner as the original data. Storing backups containing sensitive information at a non-Bureau location requires the written permission of the CEO.

(6) Data Recovery. System administrators shall develop and test procedures to restore data from backups as a contingency response to possible loss of the original data.

(7) Control of Output. Sensitive output shall be appropriately marked, controlled, and disseminated only to authorized personnel. Documents may be marked, consistent with the requirements in Section 4.d. (1), on the first page of the material, by a notation in a covering memo, by inclusion in a category identified by the Director or an Assistant Director as "Limited Official Use" and known to all personnel handling the information, or by other means the Director or Assistant Director approves. (Whenever possible, it is recommended that WordPerfect and Bureau-developed software be set up to print "Sensitive-LOU" on each page.) Each division, region, office, department, branch, etc., is solely responsible for compliance with directives concerning "Privacy Act" and "Limited Official Use" printed output.

(a) In a controlled environment, which excludes unauthorized persons, local safeguarding procedures may be established and approved by the CEO to preclude proper marking.

(b) These safeguards shall provide adequate protection and will be well-understood and adhered to by all staff members working with or having access to the information. Documents removed from the controlled environment shall be appropriately marked.

Note: Do not use the term "CONFIDENTIAL" or any other National Security Information (NSI) caveat to denote handling precautions for sensitive data.

e. Processing Sensitive Data Away From the Work Site. Employees shall protect any sensitive data removed from the work site. The removal of sensitive information from the work site shall be coordinated through the ISO and PIO.

(1) Delegation. Written approval by the CEO is required for processing sensitive data away from the work site. This approval authority may be delegated to Deputy Assistant Directors, Deputy Regional Directors, Central Office Branch Chiefs, UNICOR Division Managers, and Associate Wardens. Approvals may be accomplished by a CEO-approved listing, Institution Supplement, or individual memorandum, but a list shall be established, reviewed annually, and renewed as needed. Approvals may be designated by name or position title.

(2) Removal of Sensitive Information From the Work Site. Removal from the work site of any electronic media or output containing sensitive information shall be approved in writing as described above. The description of the information and its removal purpose shall be stated and the removal shall be approved by the CEO. Sensitive information removed for transfer to another Bureau location shall be sent by certified mail or other Government-approved delivery service, with a return receipt required. Sensitive information approved for personal transport shall be given the protection normally required for that information. With the concurrence of the PIO and ISO, the person who removes and the person who releases the data shall agree upon and document the sensitivity determination of the information.

(3) Processing of Sensitive Information on Government-Owned Equipment Away From the Work Site. CEOs, Deputy Assistant Directors, Deputy Regional Directors, Branch Chiefs, UNICOR Division Managers, or Associate Wardens shall approve the processing of sensitive information on a Government-owned PC and peripheral equipment at an employee's home or during official travel. Each approval shall be in writing, with a complete description of the equipment to be removed from the work site, including FPS or UNICOR ID numbers. Approvals shall specify the purpose and location for which the equipment will be used. This too, shall be coordinated with the PIO and ISO.

(4) Use of Non-Government-Owned Equipment to Perform Government Business. The use of non-Government-owned equipment to perform Government business at an employee's discretion does not require approval, unless sensitive information is involved. In such a case, use of non-Government-owned equipment shall require the CEO's approval; all requirements for a Government-

owned computer processing sensitive information shall apply, with the exception of contingency plans. Personally owned PCs shall comply with all provisions of this policy and the system security plan for BOPNet. In addition, the owners shall install Bureau-

authorized antivirus software, and sign a statement that they are aware of all policy requirements and will remain in full compliance.

5. PHYSICAL SECURITY

a. Computer Room. The ISO shall designate any area with a SENTRY controller, communications server, LAN file server that processes/stores sensitive data, or LAN gateway or tape backup unit (sensitive) as a Computer Room. Any other area with computer equipment that is operationally or sensitive-system-critical shall be designated by the ISO as a Computer Room. Relocating devices/equipment to a designated computer room shall be considered to avoid the need to regulate numerous computer rooms. SENTRY controllers may be excluded from Computer Rooms **only** when a physical device is installed to prevent tampering or cable switching. If a qualifying device/equipment is in a caged area within an office, that area shall be designated a Computer Room. Inmate-access LANs do not require Computer Room status, but shall prohibit unescorted access by inmates.

b. Computer Room Security. Threats to Computer Rooms exist regardless of the type of data processed. Risk analysis shall identify potential threats and losses and the countermeasures required to protect against them. The minimum protective measures essential to Computer Room security shall take all such factors into consideration. For example; a room manned 24 hours a day or sufficiently monitored to preclude surreptitious and unauthorized entry would justify fewer physical barriers or alarm systems. Processing of sensitive information introduces additional threats that may require further safeguards.

Computer Rooms shall be protected from external acts directed at the equipment, personnel, or data through administrative and physical access controls such as locks and detection devices or periodic monitoring. They shall also be protected from fire, environmental hazards, vandalism, sabotage, and theft.

In an institution, any file server installed after June 15, 1993, which is not part of a network approved for inmate use, shall be located in a locked, environmentally suitable room, preferably outside the institution's secure perimeter.

In any office outside the institution, a file server must be in a secure room that is environmentally suitable and locked when staff are not present.

The physical construction of a Computer Room shall provide the maximum security possible, considering practicality and reasonable costs. Based upon the ISO's evaluation and recommendations, the CEO must weigh the risks against the security required to protect the information and equipment. If the area is frequently inspected and evidence of tampering would be obvious without unreasonable delay, Computer Room construction may be less crucial.

When Computer Rooms are not adequately protected by procedural countermeasures, they shall be constructed with true walls (solid floor to solid ceiling), shielded external cabling, no easily accessible external windows, solid-core doors, deadbolt locks with a 1-inch throw, and intrusion detection and fire alarms where necessary.

The AISO having oversight shall develop, and submit through the ISO for the CEO's approval, an Entry Authority Listing (EAL) for each Computer Room, identifying all staff authorized unescorted entry. An EAL-listed staff member shall escort all others. Other than as the Approving Authority, the Warden's name is not required to appear on the EAL in order to be authorized unescorted access.

The CEO may determine the need for additional staff and shall provide written approval once the EAL is finalized. The EAL shall be on file with the key-issuing authority and posted on the Computer Room, clearly readable prior to entry. Keys to the Computer Room shall not be issued to anyone other than the Warden and staff who appear on the EAL.

6. SYSTEM ACCESS CONTROLS

a. Access to Sensitive Data. Computer systems processing sensitive data shall have security measures to meet additional requirements, including:

(1) System User Identification. Users shall be identified and authenticated. Passwords used for authentication must comply with the requirements of Federal Information Processing Standards Publication (FIPS PUB) 112, Password Usage, or its successor. Personal passwords shall not be shared or used by any person other than the user originally issued the personal ID. The maximum lifetime of personal passwords for Bureau computer systems is 180 days. Maximum lifetime standards may be set at fewer days for specific systems.

(2) Remote Terminals and Workstations. Remote terminals and network workstations shall be identified to the system as to their location and authorized functional capabilities (terminal-

or workstation-unique), preferably through a hardware-generated identifier such as the network interface card node address or controller port address.

b. Movement of Personnel

(1) Transfer of Staff. A new user ID shall be issued at a staff member's new duty station. The ISO at the transferring location shall disable the old user ID within one working day of the employee's departure and delete the ID within 30 days. For a SENTRY ID that cannot be created at the new duty station, use procedures prescribed in c.(3), following. On the UNICOR MCS system, the old user ID shall be permanently disabled, rather than deleted.

(2) Departing Employees. The following steps shall be taken to protect critical or sensitive data from loss and shall be documented in writing:

◆ Notification of Departure. The personnel office or department head shall notify the ISO, ISO-designated AISO, and AISO for UNICOR or Trust Fund of an employee's transfer, home duty status, termination, resignation, or other separation via E-mail as soon as the effective date is known. The ISO shall be listed on the checkout/clearance sheet.

◆ Separations. For all involuntary separations and home duty assignments, the departing employee's access to all computer systems shall be immediately disabled and his/her supervisor or the ISO shall confiscate accessible media. For routine voluntary permanent separations, the employee's access shall be terminated no later than one working day following departure.

◆ Backup. The department head or supervisor, as appropriate, shall, within five working days of termination of access, back up that user's data and directories and label the media's contents, unless the disposition of data can be concluded immediately, pursuant to the following section. (For networks and mainframes, data may remain on the system until disposition.)

◆ Disposition. The departing employee's department head or office or section chief shall determine whether the employee's information should be retained. Any information to be retained, including backups and other electronic media, shall be maintained by these managers or released to another employee at the managers' discretion. The ISO or ISO-designated AISO shall be notified of the data's intended disposition and shall

facilitate data transfer (not later than 30 days). If the ISO or AISO does not personally facilitate the disposition, he/she shall be notified of the disposition within one workday.

◆ Reassignment of Resources. When a personal computer is reassigned to a person or persons without a valid need to access data previously stored on the hard drive, data shall be purged after backup is completed (see Data Removal section).

(3) Temporary Deactivation of User Accounts. The ISO shall deactivate a user account for any staff member when determined necessary to protect sensitive information and computer resources. Written authorizations are necessary for permanent deactivations (while the user is still employed onsite) and shall be approved by the CEO.

c. Access to DOJ Data Center. Bureau employees who access SENTRY, HRMIS, FMIS, NFC, and other systems through the Department of Justice Data Center must comply with the provisions of this section (except for the UNICOR APECS system, which is isolated from other DOJ systems).

(1) TOP SECRET and SENTRY Extended Security System (ESS). All users accessing SENTRY or any other DOJ mainframe system shall be authenticated through DOJ's "TOP SECRET" security package. A "TOP SECRET" user ID and password are required for each user; it is an additional safeguard beyond the SENTRY Extended Security System (ESS). Additionally, a SENTRY ESS user ID and password shall be required for each SENTRY user.

(2) Issuing Authority. The ISO at institutions and Regional Offices shall create, manage, and delete "TOP SECRET" and SENTRY ESS user IDs. OIS, SENTRY Field Services shall be responsible for user IDs for Central Office, Community Corrections Offices, and authorized users at other agencies.

SENTRY Field Services shall also issue "TOP SECRET" and "ESS" user IDs with manager capabilities. The number of manager IDs issued to institutions shall be limited to seven, unless OIS specifically authorizes additional IDs in writing.

The institution or Regional AISO, based upon need and approval of the ISO, may be given "TOP SECRET" and "ESS" user IDs with manager capabilities. These staff are considered Noncritical Sensitive equivalent positions, as defined by the Bureau Human Resource Management Manual.

(3) Creating Personal User IDs. Staff who need to use SENTRY or any other DOJ data system shall request a personal user ID from the issuing authority. Requests to SENTRY Field Services for SENTRY IDs shall be submitted by the ISO or ISO-authorized AISO via BOPNet to the "Computer Security" E-mailbox, using the ISPS authorized form. When passwords are used for a computer system, they shall be managed and protected per FIPS Publication 112, Password Usage.

d. Password Integrity. Each user is accountable for password integrity. A user ID with a password is comparable to keys in a correctional setting. The password shall not be disclosed to anyone except as stated in Section 1., paragraph j., and shall be protected from inadvertent disclosure. Any violation of password integrity, suspected or confirmed, shall be reported immediately to the ISO.

e. Security of Computer Communication Links. Communications links from a Computer Room to remote locations shall be protected commensurate with the sensitivity of the information and the threat of unauthorized disclosure by an intruder or undetected modification during transmission. For general communication and for files that are encrypted prior to transfer, SMARTCOM, PROCOMM, etc., is sufficient. For communications containing sensitive data, encryption shall be used. OIS will establish any Bureau standards concerning software, including communications. All necessary communications software security functions shall be enabled for Bureau computer systems to protect sensitive information while it is being processed or transferred. Communication links shall be terminated upon conclusion of the intended purpose of the link.

The only exception to the establishment of a communications software standard is one necessary to communicate with systems managed by outside agencies, where the selection of software is at their discretion.

f. Remote Access Rules For Bureau Computer Systems. Any communications link involving a Bureau computer shall be carefully controlled. The following procedures apply to all Bureau systems other than SENTRY, BTS/OUTBOUND, UNICOR MCS, and Trust Fund ITS. Communications links between one or more computer systems designated as sensitive, or the transmittal of sensitive information, shall use encryption. Witness Security information shall not be accessed remotely. All remote access to LANs or PCs, including E-mail remote access, shall be in accordance with OIS-approved standards.

(1) Knowledge Requirement. Any staff member using personal computer communication and remote access software shall understand these functions well enough before using them that use does not pose a potential security vulnerability.

(2) Data Transmittal Between Computers

◆ Attended Operation. Data transmission where both computers require attended operation is permitted. Attended operation requires a staff member at each computer to initiate the communication link and any data transfers. Staff shall take precautions to ensure that files received are virus-free and do not violate licensing regulations. Sensitive data shall be encrypted.

◆ Unattended Operation. Unattended computers that are also unsecured may only receive data. Any unsecured computer left in "answer mode" must be running communications software that will limit callers' activities to sending files, without any access to data stored on the unattended computer. If the unattended computer is physically secured behind locked doors or protected with an access control software, data may be accessed. Sensitive information shall not be accessed without enabling encryption and a predefined user ID and password.

(3) Remote Control. Remote control, the ability to connect two computers and to control various functions of one computer from the other, is permitted to a Government-owned computer only as follows:

◆ For remote access to unattended stand-alone computers, where the computer is left in the answer mode and controlled remotely, remote communication shall encrypt all communications and use a predefined user ID and password. User IDs and passwords shall comply with the requirements of this Program Statement. Refer to OIS for encryption-capable communications software.

◆ For remote access to any LAN, OIS shall set the standard due to the critical vulnerabilities.

◆ Permission for remote access to any unattended Bureau computer system shall be granted in writing from the Deputy Regional Director, Associate Warden, Central Office Branch Chief, or UNICOR Division Manager, at a minimum. The authority for remote access shall include whether sensitive information will be processed.

◆ The ISO shall maintain a list of all systems that are accessed remotely and staff members who access them.

◆ The use of communications software for nonsensitive data transfer where the computer is not controlled remotely does not require security features prescribed for remote control. Security features shall be enabled for sensitive data transfer or remote control, as needed. The level of security enabled shall be changed as demand changes; the ISO shall be notified of changes.

g. PC Networks. Network user accounts, user IDs, and passwords shall comply with the previously discussed requirements for access control and the Networks Standards Manual.

(1) All users shall be given notice indicating that by "signing on" to a network they consent to monitoring of their activities, as well as any restrictions. This is done through an appropriately worded "sign-on" screen described as a banner. The wording may be tailored locally, but the following wording shall be included:

WARNING! By accessing and using this computer system you are consenting to system monitoring for law enforcement purposes. Unauthorized use of, or access to, this computer system may subject you to criminal prosecution and penalties. THIS SYSTEM IS NOT AUTHORIZED FOR CLASSIFIED PROCESSING.

(2) The network shall be protected at all workstation and terminal accesses, from "log on" until "log off." When the workstation is unattended, the user shall be logged off the network or protected by a security software program (see below), Windows, Norton, or similar screen saver password as approved by the Information Security Programs Section (ISPS). The potential for unauthorized access shall be limited to the extent possible. Approval for nonstandard security software shall be obtained from ISPS.

h. Personal Computers

(1) Power-on Password. All PCs processing sensitive data from the hard drive or diskette and "STAFF ONLY" devices shall be secure from unauthorized access. Security of unattended PCs may be accomplished through physical controls (locked office) or through a power-on password system that requires a unique user ID and password. If used, this system shall be an ISPS-approved software, Windows NT, McAfee Saber Menu, or Watchdog. The Bureau standard for security software, other than Watchdog or Windows NT, shall have the capability of unique ID and password

protection when booting, hard drive encryption (preferable),
timed and user-engaged screen blanking, and keyboard locking. If

physical and procedural controls have not been established to ensure sufficient safeguards are in place as determined by the ISO, security software use is mandatory.

(2) Keyboard Inactivity. All personal computers designated as sensitive systems or "STAFF ONLY" shall have software that will, after a specified period of keyboard inactivity, blank the display and require a password for further access. The maximum time of inactivity shall be 10 minutes. All Novell or Windows NT workstations shall use software requiring the network password. This shall be adequate for a staff member to leave a workstation unattended for a short period. The Bureau standard, related requirements, and exceptions are stated in the previous subsection.

(3) Exception. Personal computers that are accessed remotely and BTS PCs are exempt from the power-on password and keyboard inactivity requirement only with the following provisions:

- ◆ When unattended, the PC shall have physical safeguards, including a locked office, sufficient to preclude unauthorized access to the operating system or data.

- ◆ If the PC does not read, process, or store sensitive information from the hard drive or removable media drive, it is also exempt, provided any other systems accessed from this PC afford adequate protection.

- ◆ Nonsensitive "STAFF ONLY" PCs are not exempt unless inmates are prohibited from entering areas where these systems are set up.

7. PERSONNEL SECURITY

a. Computer System Positions. Bureau and non-Bureau personnel, including contractors, working in computer system design, development, support, or maintenance positions shall have security investigations commensurate with the highest level of information processed by the system pursuant to DOJ Order 2610.2A and the Human Resource Management (HRM) Manual. For the purposes of this policy, computer positions are categorized as Critical Sensitive or Noncritical Sensitive as defined in the HRM Manual, depending on the duties performed.

b. User Access Clearance Requirement. All persons accessing sensitive information in the Bureau or DOJ, including computer systems, shall have a security investigation started (with a case

number and schedule date)—at least a National Agency Check and Inquiries (NACI). Visiting or consulting physicians bound by the Hippocratic oath are partially exempted. These professionals may access pertinent patient records without a security investigation being initiated. Accessible systems are restricted to those containing relevant medical records.

Persons without approval to access sensitive systems or Computer Rooms shall be escorted by a knowledgeable staff member with unescorted access and the appropriate authority and background investigation. A Limited Background Investigation (LBI) is the minimum for unescorted access and inclusion on the EAL. The escorting staff member shall ensure the uncleared person does not access any features that could compromise security.

c. Computer Room Access. Bureau employees requiring unescorted access to a Computer Room shall have the clearance required for computer system positions in accordance with the Human Resource Management Manual.

d. Access Authorization. The ISO shall ensure all personnel security requirements are met before a staff member is granted access to any sensitive information, system, or Computer Room. Local personnel offices shall notify the ISO of the security investigation status for all new employees. Transferring Bureau employees and Bureau-assigned Public Health Service employees who have been employed by the Bureau continuously for at least one year do not require further assurance prior to granting access.

e. Non-Bureau Personnel. Non-Bureau personnel, including Public Health Service, volunteers, contractors, other Government employees, etc., who require regular access to a sensitive computer system shall have the minimum security investigations the Bureau requires for users in Section 7.b. Repair technicians or other contractors without a security access clearance may perform occasional work on a computer system with sensitive information, if they are constantly observed by a staff member with the required clearances. The staff member shall prevent any access to sensitive information by the uncleared person. Uncleared persons shall not work on any part of the security system of a computer or application system.

Investigative and security clearance requirements shall be addressed when specifications call for contract employees to access Bureau-owned or -managed computer systems. These requirements shall be met and all personnel security issues resolved prior to contract execution. The ISO shall coordinate.

8. ACCREDITATION

a. Requirement. Accreditation is required for all operationally critical computers and systems that process sensitive information, whether used on- or offsite. Required plans and risk analyses shall be incorporated into the accrediting process and documentation. Documentation shall be reviewed every three years, revised if necessary, and endorsed by the accrediting authority (AA). Revisions shall be initiated whenever the system's security is significantly affected by any modification—hardware, software, or procedural.

b. System Security Plans. System security plans are required for all computer systems that process sensitive information or are operationally critical. The CEO or his/her designees shall determine whether a system is critical. Comparable systems, operating in similar environments, may be included in a single plan. An automated System Security Plan form, mandated by DOJ as of January 1, 1995, shall apply to all sensitive systems slated for revisions or updates to existing plans, and to new plans initiated after that date (the form is available on the Bureau BBS and BOPDOCS). The plan, whether new or existing, shall comply with OMB Bulletin 90-08, Guidance for Preparation of Security Plans for Federal Computer Systems that Contain Sensitive Information. System security plans shall receive a documented review annually and be revised if needed. If policy doesn't exist, each newly developed plan (or plans subjected to the three-year accreditation review) shall include rules of user behavior—a developed set of rules of conduct for using each system, including the consequences for violating the rules.

c. Risk Analysis. A risk analysis shall be completed for comparable groups of sensitive PCs and networks that are not covered by risk analyses conducted on systems for which the Central Office is responsible. For these other systems, the risk analysis function of the Computer Configuration Control System (CCCS) may be used. The inventory portions of CCCS may also be used for each system, listing only the central processing unit (CPU) and software; however, an accurate inventory shall be maintained. Risk analyses shall be conducted every three years, addressing all vulnerabilities and threats.

d. Contingency Plans. Contingency plans are required for systems that are operationally critical or for which the continuity and safekeeping of information is mandated. Contingency plans are system- and location-unique, unless adequately addressed by an addendum to a larger plan. For some systems, requests for replacement systems can be submitted

through the normal procurement process, while others must be replaced without delay. Contingency plans need not be elaborate, but the level of protection necessary shall be addressed and documented. An ISPS-developed generic plan is available; however, all plans shall be completed in accordance with FIPS Publication 87, Guidelines for ADP Contingency Planning. Contingency planning is a step-by-step process; all potential scenarios shall be dealt with in writing. Plans shall be developed, maintained, and tested locally and the results documented annually. Test results shall be kept on file for five years or the life of the systems addressed, whichever occurs first.

e. Certification. When the system security plan, risk analysis, and contingency plan are completed, a certification team shall evaluate the system. The team shall consist of Information Security Committee members within the institution as selected by the Warden or staff members designated by the CEO at other Bureau locations, including the Central Office.

The certification process shall determine compliance with security policy, system security plans, and the accuracy of the risk analysis. Guidance for certification shall be obtained from ISPS.

The team shall thoroughly document the results. The ISO shall substantiate the accuracy of the completed report. Residual risks must be presented to the AA as part of the ISOs written request for accreditation.

f. Accrediting. Systems used to process sensitive or integrity-critical information, or that are operationally critical, shall be accredited. Once certification is completed, the ISO shall request accreditation from the AA as designated in the Responsibilities Section of this Program Statement. The AA may grant a 90-day interim approval to process sensitive information until completion of system security and contingency plans. Approval shall not exceed 180 days, including all extensions, and shall ensure that adequate protective measures exist in security plan form. Guidance and model documentation to satisfy accreditation requirements are available from ISPS.

g. Documentation. All documentation concerning licensing, security, and operations relevant to a particular system shall be maintained close at hand by the ISO. A copy of the documentation, including plans, risk analysis, certification, and accreditation, shall be readily available to system administrators, the ISO, and users at the site where the system

is accessed or physically located—including mainframes, networks, stand-alone PC systems, or groupings. Systems accredited at the Central Office level shall only require local administrators and ISOs to maintain the system security plans and the statement of accreditation.

9. INMATE USE OF COMPUTERS

Full compliance with this policy will ensure that the Bureau's information and the resources that process that information will be adequately protected. Inmate access to computer resources shall be determined at the local level, depending upon the resources available and supervised compliance with the following prohibitions:

1. Inmates shall never be allowed to use "Staff Only" computers, operationally critical systems, or systems containing sensitive information.

2. Inmates shall never be allowed to use computers attached to communications hardware (network cards or other means that would provide access to administrative LANs, SENTRY, BOPNet, Internet, Intranet, or modems).

3. The department head shall designate to staff member(s) the responsibility to monitor the content of inmate-access computers. If none are designated, the department head assumes full responsibility.

a. Computer Use Category (CUC). Inmates convicted of computer crimes or who used computers in the commission of their crimes are prohibited from work assignments involving computers and shall be given the CUC assignment of "Computer No."

The initial screening of inmates for CUC assignments of "Computer No" is the responsibility of Case Management staff. Case Management staff shall notify the ISO of all "Computer No" inmates and place the information in Section 6 of the inmate's Central File.

The ISO shall conduct a final review and determine whether the information justifies the "Computer No," ensure that qualifying inmates are given a "No" assignment in CUC, and monitor compliance with this requirement. The only CUC entries that are mandatory are assignments of "Computer No."

The ISO shall establish a local record of all CUC assignments and provide inmates' status for inmate details within seven work

days of requests. All requests for inmate clearances shall be initiated and responded to in writing.

b. Physical Controls. Control of central processing units (CPUs) and output will be done through routine staff supervision or by physically securing the equipment.

c. Application Development. Inmates shall not be allowed to develop information processing applications. Inmates are prohibited access to compilers (Turbo Pascal, Quick C, etc.) and interpreters (BASIC, BASICA, GWBASIC, etc.) that enable programs to be converted to a form the PC can execute.

d. Data Entry. Inmates may perform data entry and retrieval using software such as dBASE, WordPerfect, and Lotus 1-2-3, but may not write applications using these products.

e. Document Scanners. Inmates detailed to scan documents shall not have access to Bureau-sensitive, Limited Official Use, Privacy Act-protected or other Government sensitive information. Inmates shall not have, in conjunction with scanned documents or electronic files, access to software that can manipulate or move scanned signatures.

f. Utility Software. Software that can permanently erase, modify, or hide files (e.g., Norton Utilities, XTREE, PC Tools) is prohibited for inmate use except as needed for computer repair/assembly operations and refurbishing.

g. Computer Repair and Vocational Training Program. Under no circumstances shall an inmate repair or refurbish institution PCs or peripherals, including add-on boards, printers, monitors, or the system unit itself. Inmates assigned to a UNICOR computer repair operation or refurbishing vocational training program may repair or assemble APECS, MCS terminals, or non-Bureau computers.

Inmates may be trained to use utility software to facilitate refurbishing, repair, assembly, or quality control to produce an efficient system. Training in the use of utility software shall be conducted at the computer repair site on an as-needed basis, and shall not be offered to inmates outside the parameters described for a computer repair operation. Computer repair operations shall meet the following criteria, at a minimum:

(1) The repair area shall be isolated from all other institution/factory areas by solid walls and ceilings.

(2) Hardware and software shall be rigorously controlled.

(3) Staff supervising repair operations shall be knowledgeable about all operations to be performed and Bureau policies and local directives.

(4) Once sealed for shipping, packaged equipment shall be secured in an area where unsupervised inmates are prohibited.

h. Task-Specific Configuration. Inmates shall be allowed access only to hardware and software needed for the specific task to be performed (task-specific configuration). Access to DOS may be authorized if executable files and programs not necessary for normal operation are removed or restricted.

i. PC Security Software. It is preferred that all inmate access stand-alone PCs used in a work detail shall have Windows NT as the operating system. Existing Watchdog PCs may continue to operate with Watchdog until they are no longer functional. Windows NT or Watchdog PC Data Security shall be used to protect all hard drives that inmates use, except for systems used strictly for educational purposes, read-only devices, and LANs approved for inmate access. The access for inmates using Windows NT-protected workstations shall be restricted to what the inmate needs to perform an assigned task. Where a server connection exists, access will be managed from that point. The FPPOS automated inquiry machine and other computers where access is task-specific, computers limited to read only, inmate LAN servers, and workstations without hard drives are exempt from the Watchdog requirement (unless required by an Institution Supplement). Non-DOS/Windows NT PCs in inmate areas shall have comparable protection if inmates are prohibited from accessing all or any part of the system.

(1) Where Watchdog installation is required, the MAXIMUM Security Configuration option and area permissions shall be used. Functions, software, applications, or any areas not needed to perform assigned duties shall be restricted from inmate access.

(2) Watchdog and Windows NT on inmate-access computers shall be configured to require each inmate and staff member to have his/her own user ID and password, and shall limit access to the directories, programs, data, and computer resources required to perform approved tasks. The inmate's register number shall be assigned as the user ID. Inmates and staff shall logon with their own user ID and password. Keying under another user's ID is restricted to maintenance purposes by technical personnel with the ISO's approval. The password shall be changed upon completion of maintenance if the original was disclosed.

(3) Watchdog and Windows NT on inmate-access PCs shall be configured to prevent inmates from accessing any serial or parallel ports not needed to perform authorized tasks. Staff-only PC Watchdog and Windows NT installations shall prevent inmate access to any part of the operating system or software.

(4) Since only a single system administrator (SA) password exists on a Watchdog-protected PC, the SA password for each installed copy of Watchdog shall be recorded, sealed in an opaque envelope, and stored in a GSA- or ISPS-approved security container. A system administrator may use the same SA password on several Watchdog installations. Where only one system administrator exists (and subsequently one SA password), the same procedure shall be used.

Watchdog SA passwords may be given to alternates, provided the primary and alternates are assigned separate user IDs and passwords, and the SA function is accessed after the personal ID logon. The SA password becomes an access password and can be distributed to all who are authorized SA duties. Windows NT passwords shall not be shared.

(5) When restoration of access to Watchdog-protected hard drives becomes necessary, the ISO shall contact the Bureau's SPM/CSPM for instructions. Instructions for SA password retrieval may be obtained from Watchdog Technical Support at Fischer International (1-800-653-1811).

(6) Watchdog SAs shall have a separate user ID assigned. SA functions shall only be accessed after logon with a personal user ID and password.

(7) The Office of Information Systems (OIS) shall provide guidance and technical support on Watchdog installations and configurations.

(8) Watchdog IDs may be reissued only with the stipulation that the associated password shall be changed.

(9) When Watchdog or Windows NT is incompatible with the system requiring protection, another software package shall be procured to provide equivalent features. The ISPS shall approve all non-Watchdog (other than Windows NT) access control software use prior to acquisition, or unless selected from an ISPS-approved list.

j. Staff Access Only vs. Staff and Inmate Access PCs. A distinction shall be made between computer systems and printers

that are staff-access only and PCs that inmates also use. Institution PCs, terminals, workstations, and printers shall be clearly labeled "INMATE ACCESS" (blue) for systems to which inmates are authorized access. PCs accessed by inmates as part of UNICOR repair operations and vocational training (VT) for refurbishing are exempt. Labels shall be adhered to the equipment and clearly visible to the user, as well as all persons close by. Computers lacking "INMATE ACCESS" labels are restricted to staff only, except as stated previously. PCs, terminals, workstations, and printers with access to SENTRY or sensitive information may optionally be labeled "STAFF ONLY." "STAFF ONLY" labels are no longer required. "INMATE ACCESS" labels shall be destructible, and may be procured from UNICOR once the ISPS supply is exhausted.

k. Control of Media

(1) Disk Control. Removable media, including diskettes, tapes, etc., shall be under strict staff control; inmates shall be under surveillance when possessing them. Read-only media are excluded. When inmate use of removable media is required (preparing backups, workstation booting, etc.), use shall be under direct, constant staff supervision; the supervising staff shall be sufficiently technically knowledgeable to perform the task. An inmate may be allowed personal possession of media without constant supervision to perform assigned duties or participate in occupational training and education, if a viable accountability method is used to preclude loss, or diskettes are physically secured in the system. Accountability procedures shall be tested for functionality, certified, and approved by the ISO prior to implementation. If reliable accountability cannot be shown, the procedure shall not be used. Routine supervision is required if procedures are approved. Electronic media not compatible with Bureau computer systems are exempt.

Inmates may neither receive disks, tapes, or other electronic media from outside sources (except authorized audiotapes), nor mail them out of the institution.

(2) Hard Drive Requirement. Since the use of PCs that depend on floppy disks as their only storage medium increases the potential for abuse, new PCs (not used exclusively for LAN workstations) shall contain hard drives if purchased after 6/15/90 and existing PCs shall be upgraded, when possible, by installing hard drives. Computers used for network workstations are exempt.

(3) Printouts. While non-sensitive computer printouts may be authorized for inmate possession, inmates shall not use computers for personal needs such as correspondence or legal work without the Warden's written authority (on a case-by-case basis). This is not intended to restrict inmates' involvement in legal activities. Printing of materials not required for education courses or not specifically approved in advance shall be considered "unauthorized use of equipment" and may subject the inmate to disciplinary action. The inmate's computer-use supervisor shall ensure compliance. Printing by an inmate shall only be performed on an "INMATE ACCESS" printer. Inmates shall not have access to printouts produced by SENTRY or "STAFF ONLY" printers, unless screened and signed off by knowledgeable staff.

1. Occupational Training and Education Programs. Inmates may participate in computer training, including introductory training in how to operate PC hardware, DOS, WordPerfect, CAI Drafting, and business-oriented application software. Courses or classes providing instruction for computer refurbishing, computer repair, or assembly shall abide by the same requirements as in Section g., Computer Repair and Vocational Training Program. Since the use of computers by inmates for occupational training, recreational assessment, and education does not constitute a significant threat to the security or orderly running of the institution, CUC assignments for computer use are not applicable, unless directed by Institution Supplements.

(1) Training providing instruction in virus development or introduction, programming techniques, formula languages, or macros is prohibited. This does not preclude instruction in software such as word processors or spreadsheets, as long as such instruction does not teach programming (except in theory).

Inmates may be trained in spreadsheet design for academic purposes. In addition, due to the close relationship between dBASE commands and programming, only dBASE IV in Command Center mode shall be used in education classes. No dBASE commands may be taught.

(2) The Education Department shall request approval and submit the curriculum for all computer-related training through the institution ISO and CEO to the regional ISO prior to initiating instruction. The regional ISO shall review requests for inmate computer and electronics training programs for compliance with this Program Statement, including correspondence courses, contract courses, college courses, etc. The regional ISO shall provide a written statement of compliance with (including stipulations) or deviations from this Program

Statement to the requester. Guidance may be obtained from the ISPS.

(3) Inmates may participate in education programs that use computer-based training without approval, including literacy, ESL, and similar programs which provide instruction by computers. Training in the use or understanding of computers, telecommunications, or electronics requires approval.

m. Electric/Electronic Typewriters/Word Processors.

Typewriters and non-programmable word processors, even those with memory, are not considered computer systems for inmate purposes (the configuration is task-specific). The only restriction concerns diskettes, which shall be controlled in accordance with this Program Statement. Neither screening nor CUC assignment is required.

n. Electronic Calculators, Dictionaries, Etc.. Electronic devices approved in accordance with the Program Statement on Inmate Personal Property do not threaten the orderly running of the institution, unless they are used in conjunction with Bureau computer systems. Their memory and data storage capabilities do not necessarily exclude them from inmate possession. These devices shall be excluded if they can be used to manipulate institution data or computer systems. The compatibility of these devices with Bureau printers may create a threat to the institution if not properly controlled. Inmates are prohibited from connecting any personally owned devices to Bureau equipment.

o. Prohibited Publications. Magazines, books, and other publications that provide information on the computer underground are prohibited from inmate possession. An updated listing of prohibited publications is periodically distributed by ISPS. Publications that are not listed as prohibited or posing a threat to the secure running of a facility shall be screened for electronic media, then released to the inmate minus the media. Other publications that are determined to pose a threat to information, systems, or institution security may be prohibited by institution supplement.

10. SOFTWARE. Only Government-procured/approved software shall be used on Bureau computers, except involving computer refurbishing VT. In any case, the use of personally owned software or shareware is prohibited unless approved in writing by the ISO. The legitimate use of personally owned software on a Government computer must be justified and comply with copyright restrictions. The ISO shall be notified prior to the installation of all software, regardless of how it is acquired. An exception is authorized for legitimately acquired software by computer refurbishing VT and when obtained by OIS or CSMS specifically for evaluation and testing.

a. Software Licensing. Staff shall abide by licensing agreements with regard to copyrighted software. Offsite use of licensed software purchased by the Government is allowed only if permitted by the license. If the Government contracts for custom-made software, staff shall abide by any restrictions.

b. Software Development. Bureau-developed software shall include administrative, physical, and technical security measures in its design. The SPM/CSPM (or the UNICOR Information Security Officer for UNICOR software) shall approve security requirements prior to starting formal development of software intended for Bureau-wide use.

Design reviews and system tests shall be conducted to ensure the system is secure, and that data are protected from loss, corruption, or inaccuracy. A certification of the results shall be recorded for all new software and for existing software when significant modifications are made.

Where feasible, Bureau-developed or WordPerfect software should print "Sensitive-LOU" on all output pages that fall into these categories.

c. Software Distribution. OIS-authorized Bureau staff who distribute software shall include documentation of purchase and license agreements. If distributed electronically, documentation shall be mailed to the recipient prior to distribution.

d. Software Accountability. A system of software accountability ensures that Bureau software is installed and used in compliance with copyright laws and license agreements. The system ensures a complete, accurate inventory of software, establishes procedures for regular reviews, and institutes management controls. CCCS or another electronic database may be used to record the initial and annual inventory of software installed on all PCs and networks. Between inventories, a hard copy file system may be established for any system after conducting the initial or annual inventory in a database. Legitimately acquired evaluation software copies are exempt, provided the installation does not exceed the evaluation or testing period.

Unless otherwise directed by the ISO, the department, branch, or office in which the computer systems are managed or located shall be responsible for hardware and software inventories. Inventories shall be managed at the lowest possible organizational level by qualified staff. The ISO shall approve inventory management practices.

The following procedures constitute the Bureau Software Accountability System including credit card purchases:

(1) PC Users. When preparing a Request for Purchase (RP) for software or hardware, the requestor shall indicate the name

and location of the ISO or ISO-designated AISO to be notified when the software or hardware is received. When a documented request is not required, the ISO or ISO-designated AISO shall be consulted to ensure the items meet Bureau standards.

(2) Warehouse/Receiving Staff. Warehouses and other receiving units shall establish procedures to ensure that the ISO or ISO-designated AISO is notified of the arrival of hardware and software. Notification shall be communicated to the ISO/AISO for the cost center indicated on the original RP. Software and hardware shall not be delivered until authorized by the ISO/AISO.

Copies of purchase-related documents shall be forwarded to both the requesting individual and the ISO/AISO authorizing delivery. Documents shall include copies of purchase orders and receiving reports. Documentation regarding software purchased by credit card shall be treated in the same fashion.

(3) ISO/AISO. When notified of the arrival of software or hardware, the ISO or ISO-designated AISO shall notify the requesting individual and obtain the FPS or UNICOR Property Identification Number and serial number of the computer(s) on which the software is to be installed. The FPS or UNICOR ID and serial numbers for new computers shall be obtained from the warehouse or receiving unit.

Upon installing software or hardware, the ISO or ISO-designated installer shall update the inventory database or the individual hard copy file system with identifying information. The ISO may, based on user expertise, allow a user to install software.

When software is "uninstalled" or transferred, the ISO, ISO-designated AISO, or individual maintaining the inventory shall update the database or hard copy file using information received from the user or person responsible for "uninstalling" the software. Staff shall not "uninstall" software without informing the person responsible for the inventory.

With the exception of use for evaluation purposes, as described earlier, hardware or software may not be installed, uninstalled, or removed without the permission of the ISO or ISO-designated AISO.

(4) Documentation and Records. The department or office to which computer systems are assigned shall retain original software media and documentation (or they shall be maintained by the ISO). The designated individual within the department or

office shall maintain records pertaining to software currently installed on the computer(s) for which they are responsible. Records shall include, if possible: a copy of the original purchase order noting receipt, software license agreement, original installation diskettes (if applicable), and any existing documentation that specifies the software is assigned to a particular computer system. Purchase orders shall be noted with the identity of the intended computer system for each item. The ISO may retain these records in a central location.

(5) Software Transfer. If a PC user needs to transfer software to any other computer or storage device, he/she shall send a request to the ISO or the ISO-designated AISO by memorandum or E-mail. Once the request is approved, the user shall notify the person responsible for software inventory of the FPS or UNICOR ID of the computer to which the software has been transferred. Required documentation shall accompany the transfer, with changes noted.

(6) Outdated Software Distribution. Software that is outdated or no longer of use shall be transferred to the ISO for destruction or other legitimate disposition. Some software upgrade licenses require that the original software be retained.

(7) Audits. Departments or offices shall conduct annual audits of software; documented results shall be forwarded to the ISO, who shall review the audits of a minimum of **two** departments or offices per year.

11. COMPUTER VIRUSES. Viruses are programs designed to damage electronically stored information. To identify and contain viruses and to prevent loss of data, the following procedures shall be implemented.

a. Virus Scanning. When in use, every stand-alone PC, workstation, and server shall be scanned using a commercial virus scanning program at least daily, and whenever any new software is introduced. Stand-alone PC scanning may be automated or a terminate-stay-resident (TSR) shall be installed. This includes any and all systems used to conduct Bureau-related business: laptops, non-Government owned equipment, etc. Antivirus protection for systems connected to BOPNet shall comply with OIS standards.

PC and network antivirus protection shall be installed, updated, monitored, and managed, whenever possible, at the network level using Bureau-licensed software. Workstation PC hard drive scanning shall be performed by the network. All

network workstation hard drive antivirus installations and updates shall be conducted from the server.

b. Suspected Viruses. Any user who suspects that a computer has become infected by a virus shall contact the ISO or AISO immediately. The user shall stop work on the suspect computer pending ISO or AISO action. **Leave the computer on!** (Evidence of the virus may be lost if the machine is powered down.) Note the symptoms and record any messages that appear on the screen. Get the assistance of the network administrator to disconnect from the network. Removable media used with suspect computers shall be released to the ISO or AISO for disposition. Staff shall not alter or erase files on a suspect computer or removable media. **Allow only the ISO or ISO-authorized assistants the access needed to alleviate the problem.**

c. Virus Containment and Removal. The ISO or ISO-designated AISO shall help staff identify and contain suspected viruses, and shall use a scanning package to check potentially infected media. If a virus is found, the ISO or AISO shall:

(1) After containment or isolation of the virus, immediately notify SPM/CSPM via phone or E-mail.

(2) Notify ISPS, with a copy to the CEO and regional ISO, using the approved format via BOPNet to "COMPUTER SECURITY" within one working day.

(3) Use a current, licensed copy of an antivirus program to attempt repairs on affected computers and media.

(4) If the virus is successfully removed, release the computer for staff use.

(5) If the program cannot remove the virus, notify PC Support in Central Office; the infected computer shall remain out of service pending corrective action. Infected media shall be forwarded to ISPS or OIS upon request. **Possession of media containing viruses shall be restricted to the ISO or ISO-designated AISO only.**

d. Scanning Prior to Processing. All computers, hard drives, diskettes, CDs, etc., entering a Bureau facility or received from any source, Bureau staff or not, shall be scanned for viruses prior to use within that facility. When feasible, all data downloads from electronic bulletin boards, online systems, and other non-Bureau systems shall be executed to a diskette, which shall be scanned prior to further system introduction.

12. INFORMATION AND COMPUTER TRAINING FOR STAFF

a. Inmate Supervision. All staff shall be trained and knowledgeable about any information, system, or application used by inmates they supervise.

b. LAN Administrators. The primary, and, where feasible, assistant LAN administrators shall be trained and issued a certificate of completion to administer the system for which they have responsibility. LAN administrators shall receive training on all critical applications. All primary LAN administrators shall be scheduled within 90 days and receive training within six months after this policy becomes effective. New administrators shall be scheduled for training within 30 days after appointment and trained within 90 days.

c. Security Training. Users shall be trained in protection of computer hardware, software, and information. This includes all persons employed by or working with the Department of Justice receiving direct or indirect compensation or none at all (Public Health Service staff, contractors, volunteers, interns, persons representing or detailed from other Government agencies, etc.). They shall be made thoroughly aware of security and contingency plans for systems they use.

Any person accessing Department of Justice or Bureau computer systems shall fulfill the requirements for computer security awareness training.

(1) Instructors. Trainers must be knowledgeable on the subject and capable of conveying the essential information. Computer Based Instruction (CBI) may substitute for a qualified instructor, provided the required content is presented.

(2) Initial Training. Initial awareness training shall be completed for all employees within 60 days of their appointment and shall be consistent with NIST PUB 500-172. At least two hours of training is required. Any reasonable combination of various teaching and learning methods is authorized to satisfy time requirements. Initial training for institutional staff is conducted at the Staff Training Academy, Glynco, GA.

(3) Lesson Plans for initial and annual training shall be tailored to specific Bureau locations. There shall be two lesson plans developed at the national level; one for the institutional environment and one for the normal office environment. The latter shall be used at the Central Office, regional offices, community corrections offices, Staff Training Academy, Management

and Specialty Training Center, and any other non-institution offices. These plans may be tailored further to meet local training considerations.

(4) Initial Training Content shall include:

- ◆ Threats, vulnerabilities, and risks associated with the information and/or systems to be accessed.
- ◆ What requires protection.
- ◆ Information protection and accessibility, handling, marking, and storage considerations.
- ◆ Physical and environmental considerations necessary to protect the system.
- ◆ System, information, and access controls.
- ◆ Contingency plan procedures.
- ◆ Secure configuration control requirements.
- ◆ Responsibility to promptly report security violations to the ISO.

(5) Local Training Procedures. Prior to the issue of IDs and passwords, recently transferred and newly reporting staff shall receive a minimum of 45 minutes of locally tailored training for familiarization with institution information security, systems operation, and contingency plan procedures, regardless of training received at previous assignments. This training shall be conducted and documented by department or office staff.

(6) Continuing Procedures. Training in new computer security procedures or systems shall be provided when there is a significant change in systems' security environment or procedures, or when an employee enters a new position that requires using dissimilar systems. A minimum time for instructional purposes is not prescribed.

(7) Annual Training. Annual training shall be designed to meet employees' security awareness needs as they relate to duties and work environment. At least 45 minutes shall be dedicated to areas of information and computer security training. At Bureau locations where national security information is stored or processed, an additional 15 minutes is required for information security to address that area. Minimums may be exceeded to meet local training requirements. The SPM shall approve all training plans developed at the national level.

The information presented during annual training shall be aligned as closely as practical with the audience categories in NIST PUB 500-172. All staff shall receive training specific to their systems environment.

c. Training Record. All information and computer security training received shall be documented separately in a training information system.

GLOSSARY

Access. Capability and opportunity to view, possess, or alter information or material, including ability and means to communicate with (i.e., input or receive output) or otherwise make use of any information, resource, or component in a computer system.

Access Control. Limiting access to the resources of a computer system only to authorized programs, processes, or other systems.

Access Passwords. Passwords used to protect private or shared data; known only to the individual(s) authorized the same access privileges to that data.

Accreditation. A formal declaration by an accrediting authority that a computer system is approved to operate in a particular security mode using prescribed safeguards. The accreditation statement places responsibility with the accrediting authority and shows that security concerns have been addressed.

Accrediting Authority. Also "accreditation authority." The official who decides whether to accept or reject security safeguards prescribed for a computer system, and issues an accreditation statement or certificate prepared by the ISO that documents the decision for facilities under his or her purview. Chief Executive Officers are accrediting authorities by virtue of this Program Statement.

Administrative Controls. Management constraints, operational procedures, accountability procedures, and supplemental controls established to provide an acceptable level of protection for sensitive data.

Application System. Programs or sets of interrelated programs and data that capture, manipulate, and produce data in support of specific needs.

Assistant Information Security Officer (AISO). A staff member appointed to assist and report to the ISO on the status of information and computer security for a specific area or system.

Audit Trail. A chronological record of system activities that is sufficient to enable the reconstruction, review, and examination of a sequence of events and activities surrounding or leading to an operation, procedure, or event in a transaction from its inception to final results.

Authentication. To verify the identity of a user, device, or other entity in a computer system, often as a prerequisite to allowing access.

Authorized Person. A person who has a need-to-know for sensitive information or system access in the performance of official duties and who has been granted a personnel access clearance at the required level, or is otherwise authorized by this Program Statement to access systems containing sensitive information. The responsibility for determining whether a prospective recipient is AUTHORIZED rests with the person who has possession, knowledge, or control of the information involved, not with the prospective recipient.

Automated Decision-making System. A computer application that provides action authorization based on data input, without staff review.

Certification. Comprehensive evaluation of the technical and nontechnical security features of a computer system and safeguards, made in support of the accreditation process, that establishes the extent to which a design and implementation meet specified security requirements (system security plans).

Classified. Information that has been determined, pursuant to Executive Order 12958 or a successor order, to require protection against unauthorized disclosure and is so designated. The classifications TOP SECRET, SECRET, and CONFIDENTIAL are used to designate National Security Information (NSI), which is referred to as classified information. This Program Statement does **not** prescribe procedures for processing **classified** information.

Computer. Synonymous with Computer System or System.

Computer Resources. Any part of, or support for, computer systems, hardware, peripherals, software, firmware, programs, electronic media, or data.

Computer Room. An area with a SENTRY controller, a sensitive LAN file server, or a LAN gateway designated by the ISO as a Computer Room. Any other area with critical computer equipment designated by the ISO as a Computer Room. Computer Rooms require special security measures.

Computer Security Act of 1987. Public Law 100-235, which prescribes computer security requirements for the Federal Government.

Computer Security Program Manager (CSPM). Central Office employee appointed by the Director to develop, implement, manage, and monitor the Computer Security Program nationwide.

Computer System. An assembly of telecommunications systems or computer hardware, software, and firmware configured to automate calculating, computing, sequencing, storing, retrieving, displaying, communicating, or otherwise manipulating data, information, and textual material. A computer system is programmable. See **System** and **Telecommunications**.

Computer System Security. The combination of technological and administrative measures and controls necessary to reduce the risk of accidental or intentional unauthorized disclosure, modification, or destruction of data or system resources to an acceptable level. Includes consideration of all hardware and software functions.

Confidentiality. Protecting data from unauthorized disclosure. Not to be confused with the NSI classification "CONFIDENTIAL".

Contingency Plans. Plans for emergency response, backup operations, and post-disaster recovery maintained by a computer facility for each system as part of its security program.

Copyright Laws. Laws that protect property rights to published materials. Most software is protected under copyright law, and cannot be copied, except as clearly allowed by its license.

Countermeasures. Controls or security applied to known vulnerabilities.

Data Communications. The transfer of information from one computer to another. See **Telecommunications**.

Data Processing. The act of using data (factual information) for making calculations or decisions.

Degauss. Destroy information contained in magnetic media by subjecting them to high-intensity alternating magnetic fields.

Degausser. Electronic device that generates a magnetic field for degaussing magnetic media.

Department Security Officer (DSO). Single authority within the Department of Justice responsible for DOJ security programs.

Dumb Terminal. Computer equipment without permanent data storage or processing capabilities, which can receive data from and send data to a remote computer, and display the data received or about to be transmitted.

Encryption. Transforming data to an unreadable form in such a way that the original data cannot be obtained without using the inverse decryption process.

Environment. External procedures, conditions, and objects that affect the development, operation, and maintenance of a system.

File Server. Personal computer operating as a central data and program storage device on a local area network. See **Server**.

Identification (ID). Process that enables recognition of an entity by a system, generally by the use of unique machine-readable user names.

Information Resources Management (IRM). Planning, budgeting, organizing, directing, training, promoting, controlling, and management activities associated with the burden, collection, creation, use, and dissemination of information by agencies. Includes the management of related resources, such as Federal information processing resources.

Information Security Officer (ISO). A staff member appointed by the CEO, or the director of a geographically separated location, to manage the information security program for an area of responsibility within the Bureau.

Information Security Program (ISP). A program implemented to ensure that the processing and handling of sensitive information, in all forms, effectively protects the rights and privacy of individuals and safeguards the Bureau's operations and mission.

Legally Licensed Software. Software for which the Government or an individual has purchased or granted the right to use pursuant to the publisher's license agreement.

Local Area Network (LAN). Computer system comprised of personal computers connected to and communicating with each other through a nearby server. Enables computers to share files, gateways, printers, etc.

Media. A means for recording information which is intended to store, convey, accomplish, or transfer through hard copy (paper-based), electronic (e.g., diskette, hard drive, CD, optical disk or tape), or by any other device.

Need-to-know. Necessity for access to, knowledge of, or possession of information required to carry out official duties.

Network. System of hardware and software components whose function is the transmission of information from one point of processing or storage to another.

Offsite. Location physically detached from that in which the primary processing of data occurs. The offsite location shall not be reasonably subject to the same degree of major threat during a period in which the primary location would be threatened. If the threat is identical, additional countermeasures must be implemented.

Operationally critical. Systems where the loss of availability, data integrity, security, or rapid recovery capability would have an unacceptable or disastrous effect upon the operations of the facility. System functions necessary to the well-being of the facility could not be sustained by other methods.

Overwrite procedure. Process that removes or destroys data recorded on a storage medium by writing patterns of data over, or on top of, the data.

Password. Protected and private character string of 4 to 12 characters used to authenticate an identity.

Personal Computer (PC). Small general-purpose computer designed to support a single user at a time. Disk drives, printers, and other equipment associated with the personal computer are considered part of it. This includes "laptops," docking devices, or other portable computer systems.

Personal Password. Character string used to authenticate personal identity. Personal passwords shall be known only by the individual having that identity.

Personal User ID. Character string used to identify an individual authorized user.

Personnel Security Access Clearance. Administrative determination that an individual is eligible, from a security point of view, to access sensitive information of the same or lower category as the level of the access clearance being granted.

Physical Security. Application of physical barriers and control procedures as preventive measures or countermeasures against threats to resources and information.

Purge. Removal of data from storage devices so that there is assurance (proportional to the data's sensitivity) that it cannot be reconstructed. Purging is used when the secure physical environment will not be maintained. Media scheduled to be released from a secure to a non-secure facility must be purged.

Remote Terminal. Computer equipment transmitting or receiving data not in the immediate vicinity. This may be a "dumb terminal" or a personal computer. Remote terminals are identified to the system accessed. A modem connection is not normally considered a remote terminal unless the connection communicates directly with the server and is identified by the server without using an intermediate system as its means of connection.

Residual Risk. Risk that remains after security measures have been applied.

Risk. Probability that a particular threat will exploit a vulnerability of a system.

Risk Analysis. Identifying security risks, determining their magnitude, and identifying vulnerable areas needing additional safeguards.

Security Programs Manager (SPM). Manager and liaison for all DOJ-mandated non-custody Bureau security programs.

Sensitive System. Computer system that processes/stores sensitive data or is critical to operations (operationally critical) or a secure environment, whether or not it processes sensitive data. If a system failure would severely restrict or deny essential services or productivity, this system shall be designated sensitive. Systems that must be available to ensure the integrity of information processed or stored are defined as

sensitive. Other than "Inmate Access," all Bureau computer systems are presumed to be sensitive unless otherwise verified and documented.

Server. A central computer providing management services to other computers for multiple accesses and processes.

Standalone Computer. Computer system that is physically and electrically isolated from all other systems.

System. Telecommunications and automated information systems and computer systems. See **Telecommunications**.

System Administrator (SA). Individual appointed to manage the overall system and provide security management coverage for each system or grouping of systems. This includes local and national application systems.

System Security Plan (SSP). Each computer system and application system designated "sensitive" shall prepare and implement a plan for security and privacy, including the complete system description (identity), boundaries of the system, security controls, and management information. The level of effort expended in preparing security plans must be proportional to system size, criticality, data sensitivity, and number of users.

Task-Specific Configuration. When the system is configured to allow the user to access only what is needed to accomplish assigned tasks. Manipulation or data entry access is granted where explicitly authorized.

Task-Specific System. When the system is configured to perform certain tasks without allowing user intervention. The device is read-only, performs a singular task or specific tasks as selected from a menu, and the user is restricted from manipulating or making any changes to the system configuration or data. Systems may be task-specific by virtue of the installation of physical masking devices on key pads that would restrict entry to keying in personal identification numbers (PIN). A task-specific system may prompt you for a response or information, but no amount of input will deteriorate or otherwise alter its operation.

Task Server. Computer attached to a local area network that performs a specific function and is not used for general user access. In a typical network, a number of computers are attached that provide services to users. These "task servers" can be CD-

ROM servers, gateways, shared printer workstations, mail servers, backup servers, or any number of other devices. In many cases, servers access the network through a Novell account.

Telecommunications. The transmission, communication, or processing of data or information, including the preparation of this data or information by electrical, electromagnetic, electromechanical, or electro-optical means. See **Computer System and System.**

Terminal. Device, including "dumb" terminals, whose only function is to access another system, as well as personal computers or other sophisticated systems that may access other systems as one of many functions.

Threat. Capability, circumstance, or event with the potential to harm a computer system in the form of destruction, unauthorized disclosure, modification of data, or denial of service.

TOP SECRET Security Package. Software security system through which all systems at the Department of Justice Data Center are accessed.

Users. Persons or processes accessing a computer system.

Violation. Occurrence involving computer systems or media where there may be a deviation from security policy, or a compromise or unauthorized disclosure of information occurred or was possible.

Virus. Program introduced to a hard drive or removable storage media that may damage the computer or data. There are more than 3,000 known virus programs; the number continually increases. Virus symptoms may include:

- ◆ Unexplained changes in computer file sizes.
- ◆ Changes in file date or time stamps.
- ◆ Task servers cease to function without a logical reason.
- ◆ Unusual error messages.
- ◆ Unusually slow response time.
- ◆ Drive lights staying on longer than normal.
- ◆ Decreases in RAM size.
- ◆ Unusual messages or other screen activity.

Virus Scanner. Program that scans computer disks for viruses and removes them. Some programs can also repair corrupted files. Since new viruses are created daily, these programs must be updated frequently to include the "signatures" (telltale signs) of new viruses. Scanning programs vary in the number of viruses

they detect and the accuracy with which they locate. Many scanners have Terminate and Stay Resident (TSR) capability to decrease the need for constant user-initiated scanning.

Vulnerability. Weakness in a system (or system security procedures, hardware design, internal controls, etc.) that could be exploited to gain unauthorized access to sensitive information, or affect system availability or data integrity.

Wide Area Network (WAN). A set of widely separated computers connected together. When multiple LAN servers are connected, communication between all client computers is obtainable through their respective servers, e.g., BOPNet.