BUREAU OF THE CENSUS

Handbook for INFORMATION TECHNOLOGY SECURITY

NOVEMBER 1997

Contents

PART I. INTRODUCTION

Chapter 1: Overview

1.1 Introduction 6
1.2 Authority 6
1.3 Scope 6

Chapter 2: Responsibilities

2.1 Introduction 8
2.2 Department of Commerce IT Security Manager 8
2.3 Director of Information Resources Management 8
2.4 Chief, Acquisition & Security Division 8
2.5 ADP Security Branch 8
2.6 Division & Office Chiefs 9
2.7 Division Security Officer 10
2.8 User Community 11

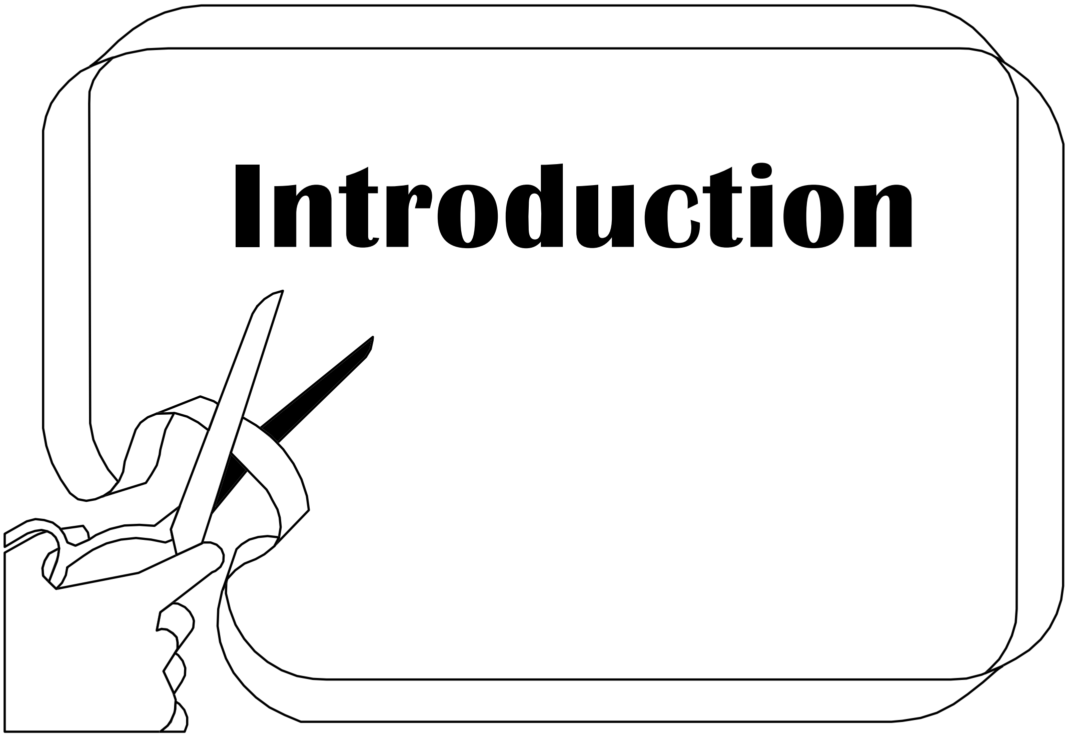
PART II. PROPER USE OF IT RESOURCES

Chapter 3: Computer & System Security

3.1 Introduction 14
3.2 Physical Access 14
3.3 Personnel Access 14
3.4 Operating System Security 15
3.5 User Account Management 16
3.6 Password Management 17
3.7 Information/Data Security 17
3.8 Software Security 19
3.9 Personal Computers 20
3.10 Portable Computers 20
3.11 Viruses & Other Rogue Software 21
3.12 Copyrighted Software 22

3.13 Personal Use of Government Computers 22
3.14 Use of Personally Owned Computer Resources............................ 23
3.15 Security Incident Reporting 23
Chapter 4: Data Communications & Network Security
4.1 Introduction 24
4.2 Telecommunications 24
4.3 Encryption 25
4.4 Electronic Mail 25
4.5 Modems 26
4.6 Remote Access 27
4.7 Internet 27
4.8 Census Public Network 28
4.9 Facsimile Machines 29
PART III. IT SECURITY PROCESSING REQUIREMENTS
Chapter 5: Systems Security Planning
5.1 Introduction 32
5.2 System Identification 32
5.3 Security Training 33
5.4 Risk Assessment 33
5.5 Establish Security Controls 34
5.6 Business Recovery Planning... 34
5.7 Certification, Verification and Accreditation 35
Chapter 6: Special Processing Requirements
6.1 Introduction 37
6.2 Processing Another Agency's Data.. 37
6.3 Processing Census Data by Another Agency or Contractor 37
APPENDIX 1: SECURITY LEGISLATION, REGULATORY POLICY 43
APPENDIX 2: DSO SIGNATURE FORM... 47
APPENDIX 3: GLOSSARY/REFERENCES 49

PART ONE



Introduction

CHAPTER 1: OVERVIEW

1.1 Introduction

Information is one of the most important assets of an organization. Protecting information and the resources that process and maintain information is critical to the continuity of operations. Security of information resources must include controls and safeguards to offset possible threats as well as controls to ensure timeliness, availability, integrity, confidentiality, etc. Information technology (IT) security encompasses the total infrastructure for maintenance and delivery of information, including physical computer hardware, supporting equipment, communication systems, and logical processes defined by software, procedures, etc.

The appropriate degree of protection depends on the value of the data processed, stored, or transmitted, as well as the cost of protecting the data. Security must protect people as well as hardware. It must provide peace of mind in a workplace that is safe and well-protected from accidents or violence. It is this added value of people protection that can make good security even more cost-effective. Security measures should be taken against unauthorized access to, or alteration, disclosure or destruction of information and IT systems, and against accidental loss or destruction of information and IT systems.

1.2 Authority

The Census Bureau strives to ensure confidentiality while providing valuable information. Data collected are typically protected by provisions of the Privacy Act and Title 13 of the United States Code, which make any release of covered data a criminal act punishable by Federal Law. Therefore employees *shall not*:

A. Use information furnished under the provisions of Title 13 for any purpose other than the statistical purposes for which it is supplied.

B. Make any publication whereby the data furnished by any particular establishment or individual under Title 13 can be identified.

C. Permit anyone other than the sworn officers and employees of the Census Bureau to examine the individual reports.

The Office of Management and Budget Circular No. A-130, Appendix III, "Security of Federal Automated Information Systems," requires the head of each Federal agency to establish and maintain an active program for managing computers and automated information. Other regulations relating to Computer Security are discussed in Appendix 1 of this handbook.

1.3 Scope

Policies are primary building blocks for every IT security effort. Policies are used as a reference for a wide variety of information security activities such as: designing controls into application systems, establishing user access privileges, performing risk analyses, conducting investigations of computer crimes, and disciplining workers for security violations.

This handbook provides a concise statement of policies and procedures related to IT security. It outlines the controls that are required to secure the IT environment and subsequently manage adequately and effectively those security controls. It should be used as a guide to implement policy for establishing proper security measures for information technology. It is intended to:

A. Acquaint employees, contractors, and consultants with the minimum required controls to protect the IT resources of the Census Bureau.

B. Clarify employee, contractor, and consultant responsibilities and duties with respect to the protection of IT resources.

C. Enable managers and other workers to make decisions about IT security which are consistent with standard policies and procedures.

D. Coordinate the efforts of different groups within the Census Bureau so that IT resources are properly and consistently protected, regardless of their location, form, or supporting technologies.

E. Provide guidance for the performance of IT audits and reviews.

This handbook applies to all divisions and offices within the Bureau of the Census that use computer systems and other IT resources for data processing and data communications. All division and office chiefs are responsible for the proper use and safeguards of any computer hardware, software, and data in their areas. The policies and guidelines set forth in this handbook are in effect for resources located at headquarters and at off-site locations.

CHAPTER 2: RESPONSIBILITIES

2.1 Introduction

This chapter is intended to provide a familiarity with the major organizational elements that play a role in IT security.

2.2 Department of Commerce (DoC) IT Security Manager

The DoC Information Technology Security Manager is responsible for the status of information technology security within the Department. The IT Security Manager is also responsible for approving the Bureau's security plans that are submitted to the Department and for the adequacy of the security programs administered by the operating units.

2.3 Bureau of the Census, Director for Information Resources Management (IRM)

The Bureau's Senior Information Resources Management (IRM) Official, currently the Associate Director for Information Technology, is responsible for the overall management of the Bureau's IT program and resources. The IT security responsibilities of the position are:

- Plan, allocate, and manage the use of IT resources to achieve Bureau program objectives at minimum expense.

- Provide a secure processing environment, including redundancy, backup, and fault-tolerance services.

- Accredit all sensitive and classified DoC IT systems that meet all applicable Federal and DoC policies, regulations, and standards.

2.4 Chief, Acquisition & Security Division

The Chief of the Acquisition & Security Division (ASD), designated as the Bureau's Security Officer, develops and directs the overall Census Bureau security program and its overall goals, objectives and priorities. Also serves as the Bureau's IT security authority.

The ASD Chief is responsible for:

- Establishing a management control process to assure that appropriate administrative, physical, and technical safeguards are incorporated into all new computer applications, any significant modifications of existing computer applications, and specifications for IT procurement,

- Assuring that IT systems security is in conformance with Departmental security policies, procedures, standards and methods,

- Assuring that stringent security regulations, policies, procedures and controls are in place for ensuring confidentiality of Census data required by Title 13,

- Maintaining the confidence of citizens that information entrusted to the Bureau will not be compromised.

2.5 ADP Security Branch

Under the direction of the Acquisition and Security Division Chief, the ADP Security Branch is responsible for the technical implementation and management of a security program that ensures the implementation of proper procedures and safeguards for protection of ADP resources and the confidentiality of program and administrative data. This includes the following functions:

- Establish and maintain organization-wide information security policies, standards, guidelines, and procedures, etc.

- Attend and represent the Bureau as a voting member of the DoC IT Security Coordinating Committee to obtain current information on issues relating to Federal or DoC IT security policies, regulations and guidelines. Also participate in special subcommittees working to resolve Departmental IT issues.

- Ensure that a Division Security Officer (DSO) and alternate is designated for each division or office.

- Establish and maintain a list of all IT systems within the Bureau and provide an up-to-date list to the DoC IT Security Manager annually.

- Ensure IT security plans are prepared in the proper format for all sensitive IT systems owned and operated by each division/office.

- Ascertain that a risk analysis is completed for all sensitive IT systems of each division/office.

- Ascertain that the Business Recovery Plans (BRP) are developed and updated for all sensitive systems of each division/office.

- Maintain a tracking system for implementing the required controls and accreditation status for all divisions/offices' sensitive IT systems.

- Act as the central point of contact for accreditation of all sensitive systems and ensure that all certification requirements are satisfied for each system prior to accreditation.

- Ensure IT verification reviews are conducted for all sensitive systems every 3 years,

- Ensure all divisions/offices are provided appropriate IT security awareness and training.

- Act as the central point of contact for all IT security-related incidents or violations. Investigate (or cause to be investigated) any incidents or violations. Maintain records and ensure reports are submitted to the DoC IT Security Manager and disseminate information concerning potential threats to system owners.

- Ensure that each division/office has procedures for dealing with malicious software (viruses and other destructive programs), along with the required virus detection/ elimination software to protect against such threats.

- Ensure that each division/office has established a policy against the illegal duplication of copyrighted software and that all systems are audited for illegal software at least annually; and inventories of all software on each individual system are maintained to verify that only legal copies are being used.

- Specify controls for firewall systems and monitoring effectiveness.

2.6 Division and Office Chiefs

Division and Office Chiefs are responsible for coordinating the security efforts of their systems. Sensitive information must be controlled to ensure protection from unauthorized disclosure, misuse, and alteration. Throughout this document, the responsibility for implementing specific controls is largely placed on the division or office chief. It is assumed that, in many cases, these responsibilities are delegated to other personnel such as system administrators, programmers or end-users. To implement this, division and office chiefs are responsible for ensuring that:

- Proper safeguards are in place for the protection of sensitive data.
- Sensitive data are never transmitted from one computer system to an unsecured/unattended environment.
- Sensitive data are never accessed by someone without the "need-to-know" and "need-to-use."
- A Division Security Officer (DSO) is designated for coordinating security regulations and requirements for the system.
- New user security orientation sessions are held in each branch to inform users of security guidelines for protecting computer and network resources such as controls for dial-up access and data communication lines and ports.
- E-mail and Internet policies are reviewed and acknowledged by all current personnel and are only utilized for official authorized purposes or else will be subject to monitoring if it is determined there are potential security breaches.

2.7 Division Security Officer

The Division Security Officer is appointed by the Division Chief and serves as the contact point between their division and the ADP Security Branch. The DSO is responsible for coordinating security regulations and requirements. These include:

- Certifying that the security requirements of their application systems are being met or will be met.
- Ensuring that the requests for accreditation of computer systems are completed and in accordance with the procedures.
- Obtaining protective measures for physical security threats such as deadbolt locks on doors, placement of electric wiring, etc.
- Ensuring compliance with all legal requirements concerning the use of commercial proprietary software, e.g., respecting copyrights and obtaining site licenses.
- Maintaining an inventory of hardware and software within the office/division.
- Coordinating the development of a Business Recovery Plan for the division and ensuring that the plans are tested and maintained.
- Ensuring completions of risk analysis to determine cost-effective and essential security safeguards.
- Ensuring preparation of security plans for sensitive systems.
- Attending security awareness and training programs.
- Reporting IT security incidents (including computer viruses) within the division to the Acquisition and Security Division, ADP Security Branch.
- Providing input to the Acquisition and Security Division, Security Services Branch, for preparation of reports to higher authorities concerning national security information.

2.8 User Community

The primary purpose of IT systems is to support the missions of organizations. Some employees use the system directly, others read reports, and others input information into their systems. These are regarded as "users," who bear a great responsibility for their systems and data.

Census Bureau employees are responsible for the adequate protection of IT resources within their control or possession, which includes:

- Protecting the confidentiality of Title 13 and other sensitive data.

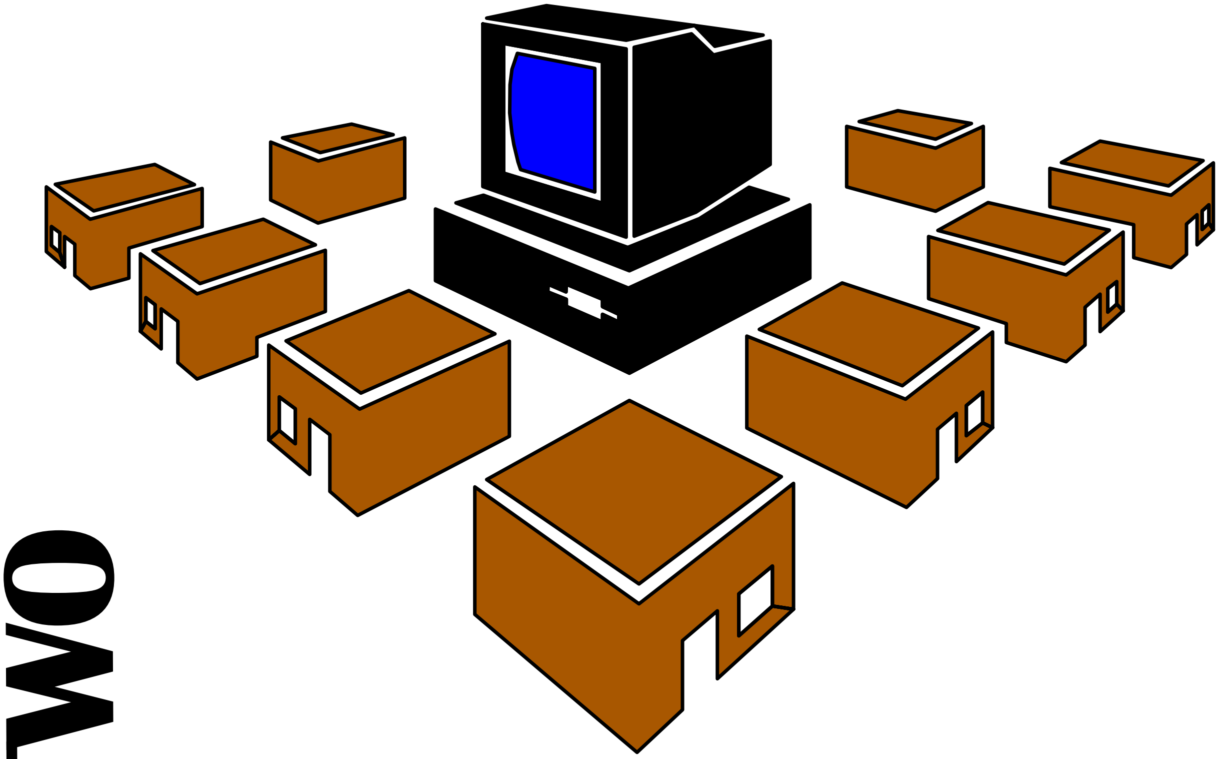
- Protecting their user (sign-on) IDs and passwords.

- Protecting their secure (access) IDs and authentication codes (passwords and PIN numbers).

- Requesting access only to applications required to perform authorized job functions.

- Using computer security controls as specified by security policies and standards.

- Using Government systems for official business only.



PART TWO

Proper Use Of Information Technology Resources

CHAPTER 3: COMPUTER AND SYSTEM SECURITY

3.1 Introduction

Computerized environments may be organized in very different ways, all of which are subject to both common and special vulnerabilities. For all processing arrangements, precautions must be taken to ensure the protection of both physical media and their contents.

3.2 Physical Access

Physical security refers to the provision of a safe and secure environment for information processing activities. The infrastructure that must be protected includes all the information processing equipment, the data it contains, and all the wiring and cabling that keep the equipment running. Physical security of IT systems requires controlling access to equipment areas where snooping, accidents, theft, or vandalism can occur. Physical security also requires protecting the IT infrastructure by providing reliable electrical power; proper temperature and humidity control; protection from fire, smoke and water, and protecting the many wires and cables upon which the systems depend. Good physical security is vital to the continuation of system processing and communication.

Guidelines:

A. All Census and non-Census personnel must wear their identification and building pass while in Census buildings so that their picture is clearly visible.

B. Protect all offices, computer rooms and work areas with key locks, cipher locks, magnetic card door locks, or other suitable access controls, if they contain sensitive, valuable, or critical information.

C. Employees while passing through doors, gates and other entrances to access-controlled areas shall not permit unknown or unauthorized persons to pass through at the same time.

D. Limit the number of entrances to the office space. Place the computer system away from the main entrances. Position work stations so there is control over who gains access to the computer system area. If a theft does occur, report it to the appropriate authority in your Division or Office and submit an incident report (BC-1206) to Acquisition and Security Division. Divisions and offices at headquarters should contact the Federal Protective Service. Regional offices should contact their local police department.

E. Properly secure computer systems to prevent theft, misuse, and abuse.

F. Supervise or challenge individuals who are neither Census employees nor authorized contractors whenever they are in a restricted area containing sensitive data.

G. Obtain an approved and signed property pass (Form BC-1550) for all computers and related information systems equipment leaving Census Bureau property. The property pass must be signed by the division or office property custodian.

H. Physically secure all information storage media such as hard disk drives, floppy disks, magnetic tapes, and CD-ROMs which contain sensitive, valuable, or critical information.

3.3 Personnel Access

Employees are the key ingredient in successfully securing a data processing installation. In many instances the employee represents the weakest link in the security chain. Most of the emergencies for which security systems are built are caused by people who are either employees or ex-employees of the organization in which the emergency occurs. It is generally agreed that there is no totally airtight security system; it is not possible to guard against all security breaches that may be caused by employees. It is possible, however, to minimize the risks either by instituting preventive measures or by early detection and correction when breaches do occur.

<u>Guidelines</u>:

A. Follow all policies, procedures, and standards governing personnel security concerning employees, contractors, and individuals with Special Sworn Status, as covered in the Census Administrative Manual (CAM) and Memorandums.

B. Ensure that employees, contractors, and individuals with Special Sworn Status undergo the appropriate type of investigative processing for suitability and security.

C. Ensure that employees and contractors, and individuals with Special Sworn Status before being assigned to sensitive positions, receive a security awareness briefing. They should be informed of their personnel security duties and responsibilities, and the possible penalties or administrative actions which may be imposed for intentional or unintentional security violations, or actions which are dangerous to security (*see Employee Handbook*).

D. As a condition of continued employment, employees, contractors, and individuals with Special Sworn Status agree to comply with information security policies and procedures (*see Chapter 6, Table 6.1*) and sign an Oath of Nondisclosure.

E. Ensure that non-Census Bureau personnel, such as contractors, researchers, or other government agency personnel who require access to Census information are processed in accordance with Personnel Security procedures and follow guidelines in Chapter 6, Table 6.1.

F. Ensure that individuals are held personally responsible for the proper use and security of the information resources under their control.

G. Return all Census Bureau property when an employee or contractor terminates their relationship with the Census Bureau. Property includes portable computers, library books, documentation, building keys, magnetic access codes, outstanding loans, and the like. These terminating individuals must inform management about all property they possess, as well as all computer system privileges, building access privileges, and other privileges they have been granted.

H. Store vital records in a secure area which is unlikely to be damaged by any event. Vital records are those which are required by statute to be retained for a specified period of time or which are essential for the performance of a major Census mission established by statute, Executive Order, or similar authority. The loss of these records could have severe consequences if it is subsequently determined that they were lost because of failure to provide adequate and reasonable protection.

3.4 Operating Systems Security

The operating system is an organized collection of routines and procedures for operating a computer. Functions performed include (1) scheduling, loading, initiating, and supervising the execution of programs; (2) allocating storage and other facilities; (3) initiating and controlling input/output operations; (4) handling errors. Whether the operating system resides on PCs, LAN servers, workstations, or minicomputers or mainframes, and because it controls system applications and functions, it is essential to have stringent access control procedures.

Access control is the process of limiting access to the resources of a system only to authorized programs, processes, or other systems. Basic controls include individual accountability; giving users IDs and passwords, and access rights; giving users access to specific objects, such as programs, activities (commands), files, or records. In order to achieve this, the guidelines listed below should be followed.

Guidelines:

A. Follow appropriate IT Standard for specific operating system.

B. Control access to objects according to the user's authorization. The system must be able to allow or deny access to objects based on the profile of the user.

C. Maintain an audit trail, at a minimum of login attempts, password changes, and file creations, changes and/or deletions. The audit trail must be protected in such a way that it cannot be changed by the user. Logs of computer security relevant events must provide sufficient data to support security reviews of the effectiveness of and compliance with security measures.

D. Review audit trails regularly and report any anomalies to the appropriate supervisory and/or security personnel for follow-up action.

E. Prevent unauthorized access by clearing all protected information on objects before they are allocated or reallocated out of or into the system. Objects being allocated into the system also must not contain residual protected data which other users may access.

F. All vendor-supplied default passwords must be changed before any computer or communications system is used for Census Bureau business.

G. Never include the word "Welcome" as part of the login process and display the following warning message prior to the system user name or password:

WARNING*WARNING*WARNING
YOU HAVE ACCESSED A UNITED STATES GOVERNMENT COMPUTER. USE OF THIS COMPUTER WITHOUT AUTHORIZATION OR FOR PURPOSES FOR WHICH AUTHORIZATION HAS NOT BEEN EXTENDED IS A VIOLATION OF FEDERAL LAW AND CAN BE PUNISHED WITH FINES OR IMPRISONMENT (Public Law 99-474). REPORT SUSPECTED VIOLATION TO YOUR DIVISION SECURITY OFFICER.
WARNING*WARNING*WARNING

H. Password protect those utilities which are required only by the installation LAN manager to maintain security files.

I. Ensure the operating system software maintains an encrypted software history of user's previous passwords. The history file must minimally contain the last thirteen (13) passwords for each user ID.

J. Mask, suppress, or otherwise obscure the password display such that unauthorized parties will not be able to observe or subsequently recover them.

K. Follow any and all related hardware standards as developed by the Standards Management Teams.

3.5 User Account Management

Authentication is a positive identification, with a degree of certainty, sufficient for permitting certain rights or privileges to the person or thing positively identified. Division and Office Chiefs are responsible for authorizing user access based on the following guidelines.

Guidelines:

A. Only Census employees and those personnel with Special Sworn Status (SSS) are authorized to obtain user accounts on any Census Bureau computer system.

B. Implement the user account naming convention on all computer platforms. Ensure that each user of Census Bureau computer systems is assigned a unique, personal user account name that will be used for systems authorization. Contact the ADP Security Branch for the division/office user account name list.

C. Authorize the creation of user accounts from the user account name list and the removal of user accounts when employees leave the division or office.

D. Make user account name requests for authorized users and non-Census users such as contractors, guest accounts, and others to the Chief, ADP Security Branch.

E. Request changes to a user account name because of an employee name change to the Chief, ADP Security Branch.

F. Ensure that the user account name list is not made available to the general public.

G. Ensure that system administrators establish and maintain user accounts in their respective areas. The initial passwords issued by a system administrator must be pre-expired.

H. Limit the number of consecutive attempts that a user may make to enter an incorrect password. After three (3) unsuccessful attempts to enter a password, the involved user-ID must be either (a) suspended until reset by a system administrator, (b) temporarily disabled for no less than three (3) minutes, or (c) if dial-up or other external network connections are involved, disconnected.

I. Automatically terminate privileges for inactive or dormant user ID's after a 60-day period of inactivity.

3.6 Password Management

Identification of an authorized user is done by means of some name or equivalent known to the system. One of the easiest and most effective access control methods is passwords.

Guidelines:

A. Make passwords at least six characters long (5 alphabetic & 1 numeric in any order). Passwords which are eight or nine characters long are preferred.

B. Change passwords on all accounts at least every 30 days.

C. Avoid names, permutations of names, and initials of spouses, children, and pets for passwords. All computer system users must choose passwords that cannot be easily guessed. A password should not reflect the account owner. Also, avoid items like a badge number, a social security number, or birth date. Passwords with special characters, such as $ and #, are recommended.

D. Do not include passwords in any files, such as the body of an electronic mail message or in a login script.

E. Change passwords immediately if you suspect that your password has been compromised.

F. Never write your password down and never give your password to any other user.

G. Make new passwords different from previous passwords, when it is time to change your password.

3.7 Information/Data Security

Information and data are important Census Bureau assets. Access to, use of, and processing of Census Bureau data must at all times be consistent with the following policy guidelines.

Guidelines:

A. Use system access controls for all computer-resident information that is either sensitive, critical, or valuable to ensure that it is not improperly disclosed, modified, deleted, or rendered unavailable.

B. Limit the handling of sensitive input data only to authorized personnel and provide an audit trail of the data as it passes from person to person or point to point in the process. This audit trail must assure personal accountability from initial receipt to distribution, storage, or destruction of the final products.

C. Clearly label containers, tape reels, disk packs, floppy disks, and similar data storage media as to contents and the sensitivity. Labelling helps prevent accidental disclosure of sensitive information, and notifies users of the need for continuous protection.

D. Prevent inadvertent destruction (e.g., overwriting), subject to the capabilities of the system, by the use of "write protect" rings, internal labels, floppy disk tabs, or similar system-specific safeguards.

E. Use static protection equipment, surge suppressors, or electrical power filters on all microcomputers and PCs to protect against risk of power surges and static electricity.

F. Store and control all sensitive data on media such as magnetic tape, disk, and similar devices in the media library when not required for processing. If a media library is not justified, as in the case of a microcomputer, the sensitive diskettes and tapes should be stored in a locked safe or cabinet with all other controls in place.

G. Notify the Chief, ADP Security Branch when sensitive data is, or suspected of being, lost or disclosed to unauthorized parties.

H. Notify the Chief, ADP Security Branch when organizational units have a new requirement to process sensitive data, and specify the security controls required for its protection.

I. Assure that appropriate security requirements are included in specifications for the acquisition or operation of new information processing equipment.

J. Clear magnetic media (tapes, disks, hard drives) containing sensitive data prior to reuse. This includes returning magnetic storage media to a vendor for trade-in, servicing, or disposal. To clear, overwrite all sensitive data, a minimum of three times, with a commercial disk utility program. If unable to overwrite, degauss using a commercial degausser (see *Census Administrative Memorandum General-16*).

K. Do not store sensitive information such that it is commingled with other data on floppy diskettes or other removable data storage media (tapes, disks, hard drives, etc.).

L. All sensitive system-generated output (electronic & non-electronic) must be properly labeled, under protection of Title 13 U.S.C. as follows:

Non-public use documents and materials not available to the public that contain information protected by Title 13 U.S.C. should be marked in bold type on each page with the phrase "DISCLOSURE PROHIBITED --TITLE 13 U.S.C."

Reports or memoranda of more than one page that contain information protected by Title 13 U.S.C. must contain the following statement on the cover page in bold type: "THIS (report, memorandum) CONTAINS INFORMATION, THE RELEASE OF WHICH IS PROHIBITED BY TITLE 13 U.S.C. AND IS FOR BUREAU OF THE CENSUS OFFICIAL USE ONLY."

M. Destroy sensitive material after it has served its intended purpose by either burning or shredding. Keep sensitive material that is too large or numerous to put into burn bags in a secured area until ready for destruction. The destruction process must prevent recognition or reconstruction of the information (see *Census Administrative Memorandum General-16).*

N. Remove all paper copies of sensitive information if a copy machine or printer jams or malfunctions while copying or printing the sensitive information and destroy as stated above.

O. Do not leave printers unattended if sensitive information is being printed or will soon be printed. An exception will be made if the area surrounding the printer is physically protected such that persons who are not authorized to see the material being printed may not enter.

P. Follow the appropriate shipping and receiving guidelines for sending private, confidential or sensitive information through the mail, by messenger or courier (see *Census Administrative Memorandums General 9 & 13).*

Q. Properly secure all sensitive information and data when it is not being used or when left in an unattended area.

R. Backup at least monthly all sensitive, valuable, or critical information resident on Census Bureau computer systems.

3.8 Software Security

Software is the heart of an organization's computer operations, whatever the size and complexity of the system. Therefore, it is essential that software function correctly and be protected from corruption.

Guidelines:

A. Prior to placing a sensitive application into operation, verify that all required user functions are being performed completely and correctly. Ensure that the specified administrative, technical, and physical safeguards are operationally adequate and fully satisfy the applicable Federal information protection policies, regulations, and standards.

B. Define security requirements and specifications to be approved by the user prior to acquiring or starting development of applications, or prior to making a substantial change in existing applications (see *IT Standard 13.0.0: Configuration Management Standard*).

C. Conduct design reviews at periodic intervals during the developmental process to assure that the proposed design will satisfy the functional and security requirements specified by the user.

D. Thoroughly test new or substantially modified sensitive applications prior to implementation to verify that the user functions and the required administrative, technical, and physical safeguards are present and are operationally adequate. This is normally accomplished as part of the certification process described in Part 3, Chapter 5 of this manual.

E Do not use "live" sensitive data or files to test applications software until software integrity has been reasonably assured by testing with non-sensitive data or files.

F. Do not place sensitive application software in a production status until the system tests have been successfully completed and the application has been properly certified as required by OMB Circular A-130, as summarized in Part 3, IT Security Processing Requirements.

G. After certification, add the sensitive applications software to the production library, to be subsequently controlled by persons other than the software developers.

H. Formally request, approve, and document changes to existing applications (see *IT Standard 13.0.0: Configuration Management*). Software changes will be made to a copy of the application software rather than the production version. The new version will be thoroughly tested to assure correct and secure operation before being placed into a production status. If substantial changes are made to a sensitive application, the application must be recertified by the appropriate official.

I. Maintain current copies of critical application software, documentation, databases, and other resources required for its operation at a secure off-site location to be readily available for use following an emergency.

J . Duplicate all utility software (which allows for duplication) and files which have taken over 40 staff hours to create. Store backup copies of vital data in a separate physical location to protect against destruction in the event of fire or other disaster. If the data are sensitive or critical, ensure that the backup copies are in a locked cabinet.

K. Retest and recertify sensitive applications every three years or following substantial changes.

L. Provide the same degree of protection to sensitive software documentation as that provided for the software.

3.9 Personal Computers

A personal computer (PC) is a single user computer system that most employees use for office automation, project work, and software and system development. These systems, when originally designed and made available in the early 1980's, offered a tremendous computing resource but very little security. Prior to the personal computer, physical security, file and data management, system backups, and recovery were managed centrally. Since there were limited networking and remote access activities, security was the primary concern of data center managers. Today, security is a concern to all users of computing technology.

Guidelines:

Observe the following practices to ensure a safe and secure computing environment:

1. Limit access to your PC.
2. Log out and turn off the PC when not in use.
3. Use locking devices to secure hardware when available.
4. Avoid leaving sensitive data in the PC.
5. Prevent unauthorized software from being installed on your PC.
6. Scan all incoming and outgoing diskettes for viruses (see *Viruses and Other Rogue Programs-Section 3.11*).
7. Label and store diskettes securely when not in use.
8. Prior to reuse, overwrite all magnetic media containing sensitive data a minimum of three times with a commercial disk utility program. If unable to overwrite, degauss using a commercial degausser.
9. Use screen savers to protect sensitive information from being displayed.

3.10 Portable Computers

Portable computers such as laptops and other devices are being used increasingly to support survey projects in the field and by employees to perform Census work while on travel or other work sites. Security requirements for these systems depend primarily on the risk of theft of portable equipment which would compromise both the system and the software and data contained within it. Another potential risk of loss to the software and data is presented when data is transmitted over unprotected communications lines, such as from home, a hotel room, a car phone, or an airport pay phone.

To determine appropriate security controls for using these systems, a risk assessment should be conducted and consideration given to issues such as the crime rate in the local area, the type and quantity of processing, the sensitivity of the data being stored and transmitted, and the communications lines over which data is transmitted.

Guidelines:

A. Perform a risk assessment to determine appropriate security controls.

B. Store the equipment in a locked container or room, such that it is out of sight and inaccessible to potential theft. This might include the locked trunk of a car, safe, or storage room.

C. If possible, store sensitive information on removable diskettes and keep them locked up when not in use.

D. Encrypt sensitive (Title 13) information/data contained on portable computers (see *Section 4.3-Encryption for Guidelines*).

E. Document the security controls and train portable computer users on these controls.

3.11 Viruses and Other Rogue Programs

Malicious software presents an increasingly serious security problem for computer systems and networks. Malicious or "rogue" software includes viruses and other destructive programs, such as Trojan horses and network worms. This type of software is often written as independent programs that appear to provide useful functions but they also contain malicious programs that can be very destructive. Malicious code can spread quickly through software bulletin boards, shareware, and users unknowingly copying and sharing contaminated data files and software products. Networks are particularly vulnerable as they allow very rapid spread of the virus to all systems connected to the network.

Computer viruses have become a threat to virtually everyone using a computer. A virus can destroy programs and data by copying itself to other programs. It is then executed when the infected program is run. It can disable computers and entire computer networks. It can also cause lost computer time and staff resources to track and eliminate it.

PCs are more susceptible to viruses than other types of computers due to their widespread use. However, viruses can be created for any type of computer. Sound IT security procedures will help detect and prevent computer viruses and other malicious programs from spreading or causing damage.

Guidelines:

A. Use updated anti-virus software to ensure the timely detection and elimination of viral infections.

B. Have authorized, properly purchased licensed software installed by system administrators *only*.

C. Train and brief all division personnel on viral detection and elimination procedures and policies.

D. Report all incidents detected or suspected immediately to the Chief, ADP Security Branch.

E. Minimize the risk and spread of viruses and other malicious software by ensuring that the following procedures are practiced:

   1. Scan personal computers and servers periodically with anti-virus software.
   2. Always scan incoming or outgoing diskettes before using.

3. Never boot the PC with a diskette unless it has been scanned.
4. Scan your PC before backups are performed and scan PC backup diskettes before restoring.
5. Scan a newly purchased PC before using or connecting to a network.
6. Scan zipped files BEFORE and AFTER unzipping.
7. Scan any files downloaded from bulletin boards or the Internet.
8. Scan program file diskettes before installing new software.
9. Use a write-protect tab on diskettes.
10. Maintain clean, write-protected copies of application software and bootable system diskettes for restoration.
11. Implement access control (read, write, and execute permissions) on files.
12. Avoid sharing diskettes.

3.12 Copyrighted Software

Software which is purchased for use at the Census Bureau must be protected from damage and theft. Copyright laws provide protection for proprietary software. The policies below guard against violation of these laws and protect the Census Bureau from system damage and unauthorized use of existing hardware and software.

Guidelines:

A. Control and protect proprietary software from compromise by not giving or lending out software.

B. Ensure hard disk drives of microcomputer (PC) and workstation users are periodically checked and inventoried to protect against copyright infringement.

C. Do not copy software unless such copying is consistent with relevant license agreements or copies are being made for archival purposes.

D. Research the software's point of origination to guard against use of pirated software.

E. Do not install unauthorized software on any computer system.

F. Obtain proper approval and authorization prior to purchasing or placing any software program on a division or office computer.

G. Establish and maintain procedures for approving computer software and keep a current inventory of authorized software for each computer.

H. Require software to meet stringent criteria before approving it for use on your computer system. Software should be carefully reviewed to prevent viruses.

3.13 Personal Use of Government-Owned Computers

Microcomputers and small computer systems are vital tools at the Census Bureau. With developments in technology, the Census Bureau has witnessed a proliferation of smaller computer systems. Proper and authorized use of a Government computer system is necessary to ensure system integrity and operational security. The Computer Fraud and Abuse Act, Public Law 99-474, was passed to provide for punishment of individuals who abuse or commit fraud on Government computers.

Guidelines:

A. Use Government computers, communications systems, and data or information for official authorized purposes only.

B. Census employees or other individuals with access to Government computers and related equipment who knowingly misuse this equipment or its output for personal, recreational, or other unofficial uses will be subject to disciplinary actions, up to dismissal and/or criminal prosecution.

C. Since the Census Bureau's computer and communications systems must be used for official purposes only, employees should have no expectation of privacy associated with the information stored or sent through these systems.

3.14 Use of Personally Owned Computer Resources

The Census Bureau has the responsibility to supply employees with office automation equipment and software for official business purposes. Bringing in personally owned equipment and software to be used for business purposes can result in many vulnerabilities and liabilities such as computer viruses.

Guidelines:

A. Do not bring personally owned data processing equipment, software, or data into the Census Bureau to be used for official business.

B. Purchase data processing equipment and software to be used at the Census Bureau through regular procurement channels.

3.15 Security Incident Reporting

A computer security incident is the unauthorized use of a computer or the use of a computer in violation of Census standards, policies, and procedures. Examples of security incidents may include, but are not limited to: use of unauthorized accounts, attempts to steal or crack passwords, placement of virus or Trojan horse programs, or misuse of government equipment. An incident may originate either from within the Census Bureau or from outside agencies and may involve the activities of Bureau employees or outside parties.

Guidelines:

A. Report all suspected IT security problems or violations to the Chief, ADP Security Branch.

B. Communicate the security incident via phone call or paper mail. If e-mail must be used, avoid revealing phrases in the subject. Words like "hackers", "incident" or suspect names can be dead giveaways to unauthorized, interested parties.

C. Ensure that every password is changed on a system that has been involved in a successful attack by a hacker or by some other system penetrator.

CHAPTER 4: DATA COMMUNICATIONS & NETWORK SECURITY

4.1 Introduction

The growth in data communications in recent years can only be described as explosive, and there is little possibility that this will not be equally true in the foreseeable future. As with other human activity, there are forces at work, both intentional and inadvertent, that can subvert these activities and cause harm to the institutions and individuals involved. Security measures must be intelligently designed and conscientiously enforced to minimize the ever-increasing risks and threats.

4.2 Telecommunications

Not too long ago, when data were processed only in batch mode, security over ADP activities was rather simple. Physical, environmental, and procedural security measures satisfied the majority of the security requirements for most data centers. However, numerous additional vulnerabilities were instantly created with the advent of telecommunications. Cables leaving the computer room can be considered a back door, giving users at remote terminals direct access to the computer. Many of the capabilities that were once reserved for a limited number of computer room personnel are now available to worldwide end users. A controlled environment is therefore more important today than ever.

Guidelines:

A. Follow all telecommunications and security requirements when transmission of sensitive data is deemed necessary. Contact the Chief, ADP Security Branch, for assistance with security planning.

B. Use dial-up communication facilities only when the need has been established, approved, and provided with the appropriate level of security. Approval for the use of dial-up communications for sensitive applications must be obtained from the Telecommunications Office.

C. Control telephone numbers for dial-up communications that are provided to authorized users. Such telephone numbers will not be publicly listed or otherwise made available to the general public. If a telephone number must be made available to users located outside the local area, these users must be made aware of this requirement and agree not to make them available to the general public.

D. Use terminal identification, dial-back, encryption, and other devices when deemed necessary to control access to automated information systems through dial-up communication facilities.

E. Ensure that the network owner establishes and maintains a level of security necessary to:

(1) adequately control network access,
(2) ensure the protection and integrity of message traffic as required by the owners of the information being transmitted, and
(3) ensure the adequate protection of network nodes.

F. Do not connect an information processing system to any network, either internal or external to the Bureau, that does not provide adequate protection for the information transmitted.

G. Positively identify and authenticate authorized users of remote processing facilities through the use of an effective password system and additional security controls as needed.

H. Restrict to authorized personnel access to telecommunications controllers, closets, frame rooms, concentrators, processors, diagnostic equipment, and circuits.

I. Ensure that reasonable care will be taken in the placement of cables forming a part of the telecommunications distribution system in order to deter tampering and preclude possible loss of data and/or the ability to communicate.

J. Fully document the design and configuration of all data communication facilities. Such documentation will be maintained on a current basis with access limited to authorized personnel.

K. Consult and obtain approval from the Chief, ADP Security Branch, if considering instituting an application gateway firewall.

L. Utilize advanced authentication for remote access to the Census Network (CENNET). Should remote access to CENNET via dial-up modems or an external network be permitted, the users must be authenticated by the firewall.

4.3 Encryption

Government agencies are required to cryptographically protect "data that has or represents a high value if it is vulnerable to unauthorized or undetected disclosure or modification during transmission or while in storage." NIST's Federal Information Processing Standard (FIPS) 140-1, "Security Requirements for Cryptographic Modules," provides a standard for Federal organizations when encryption is to be used to provide protection for sensitive or valuable data. FIPS 140-1 states that an encryption algorithm, either hardware or software, must comply with an existing FIPS or has been certified through NIST's validation program.

Guidelines:

A. Ensure that any encryption software purchased utilizes a FIPS-approved algorithm like the Data Encryption Standard (DES).

B. Use the Data Encryption Standard (DES) to encrypt when data confidentiality is required, such as Title 13.

C. Ensure that any Title 13 data transmitted to another authorized Census employee using e-mail are contained in a file attachment that has been properly encrypted.

D. Develop management procedures involving key generation, key distribution, key storage, and key destruction and submit them to the ADP Security Branch for review & approval prior to implementation.

E. Provide appropriate physical security for the protection of all encryption devices.

4.4 Electronic Mail

E-mail systems in the Bureau of the Census do not assure personal privacy unless additional procedures and technology are added to enhance the e-mail system to protect against unauthorized interception and disclosure of the message.

Sensitive data are a special type of data that includes any data collected, processed, and protected under the provisions of Title 13, Title 26 (IRS), Social Security Administration

(SSA) agreements, Privacy Act, and so forth. Reorganization information and EEO case data are two examples of sensitive data. Like all other Government computer environments, steps shall be taken to protect data sent through electronic mail.

Guidelines:

A. Consider all messages sent over Census Bureau computer and communications systems as the property of the Census Bureau.

B. Do not send sensitive data of any kind in the text of an e-mail message. This includes Title 13 data and information that must be kept private.

C. Encrypt files containing confidential or sensitive data when sending as attachments to e-mail messages. Double check your data files to be sure they are the ones you intend to transmit.

D. Ensure all e-mail messages are addressed to the intended recipient and not someone else with the same name. Also, some Census employees have user accounts on other Commerce computer systems and may appear in the cc:Mail directory more than once. Any Census cc:Mail directory address for a user account on a non-Census system will have an address suffix after the name, such as "Smith, John [Admin@OSEC]." Accounts on Census computers do not have these suffixes.

E. Employ the Bureau's password management standards when any computer system or network within the division offers e-mail as a service (see *Section 3.6-Password Management*).

F. Either lock the terminal, log out of the session, or use a password protected screen saver, when leaving the computer while still in electronic mail. Unauthorized users shall not read or send messages from another person's account.

G. Advise employees that e-mail messages communicated between internal nodes and external sources are subject to monitoring and review as is any resource provided for an employee's use. Internal nodes include any Census Bureau computer system with an e-mail capability. External sources include DOC personnel, any Government or Non-government agency, commercial or educational organizations, and individuals. Monitoring and review activities will be automated and are necessary to ensure that e-mail systems are being used appropriately.

H. Ensure that electronic mail bulletin boards are properly justified, implemented, and managed in their respective areas.

4.5 Modems

Computer systems are increasingly vulnerable to misuse due to accessibility through modems. Stringent controls for dial-up computer access are required to protect sensitive data, computer software, and hardware. These controls begin with the physical connection of the modem to the computer system and telephone. Internal modems should be disabled when not in use and external modems should be disconnected. In addition to preventing users from dialing into the computer system, concern should be given to authorized users dialing out. Once a connection is made to an outside source through the modem, the computer system becomes vulnerable to misuse by the outside user. It is essential that users have procedures for ensuring the positive identification of the unit being called.

Many personal computers are manufactured with built-in modem boards and others are equipped with an interface board for easy connection to an external modem. Both configurations are used extensively at the Census Bureau for data systems. Personal computer-based modems are permitted only on personal computers not performing data communications with any other Census Bureau computer system, file server, or disk server.

<u>*Guidelines*</u>:

A. Disconnect a personal computer using a modem from all local area networks, other personal computers, file servers or disk servers, and other peripheral equipment, prior to operating the modem.

B. Ensure that all telecommunications programs are disconnected when personal computers are not being utilized.

C. Never leave modems in automatic answer mode or unattended unless in a secured room.

D. Never leave a personal computer unattended while a remote communications session is in progress, unless the area is secured.

E. Never transmit or receive sensitive data by a modem over unprotected telephone lines. Either use an approved data encryption system or use dedicated data communication lines or both (see *Section 4.3-Encryption*).

F. Coordinate the use of data encryption methods with the Acquisition and Security Division and the Telecommunications Office if sensitive data are to be communicated via modem.

4.6 Remote Access

The term "remote access" means using any of the resources of a network (file servers, printers, workstations) from a remote location.

In certain special circumstances, access to some services within the Census secure wide area network can, at the discretion and approval of the respective division or office chief, be permitted for employees working at remote sites. Special circumstances requiring remote access to sensitive Census processing systems is considered temporary in nature, such as an employee on travel, detailed to an alternate work site, or emergency (non-routine) systems administration. This capability is not intended to allow working at home.

<u>*Guidelines*</u>:

A. Limit all requests for remote access to employees on travel or otherwise working on Census business at an approved facility.

B. Make available modem telephone numbers, connected to Census computers or networks, to Census employees ***only***. This will minimize hacking attempts and other unauthorized use.

C. Ensure that the dial-in access phone numbers are used by Census employees only and any Census computer system accessed is used for official business only.

D. Only use Government-furnished equipment to access Census computer systems remotely.

E. Make employees aware that all remote access communications are subject to monitoring.

4.7 Internet

The Internet provides Census Bureau employees access to unlimited sources of information. It has also been an excellent vehicle to inform the public about the Census Bureau's mission and showcase some of our data products to the world.

Understanding and exploiting the potential of the Internet means using and exploring its tremendous resources. However, as users of the Census Bureau's Internet interface we must always practice safe computing and protect sensitive data to keep the computers and networks secure.

Internet access, specific Internet services, and computer resources are considered corporate resources. The Telecommunications Office (TCO) will ensure that any Internet connection to Census computer systems and networks is properly protected in accordance with Census "firewall" and security policies. The Census Acquisition and Security Division (ASD) will monitor the proper implementation and effectiveness of security controls continually to ensure secure use of the Internet.

Guidelines:

A. Division and office chiefs, at their discretion, shall grant employees Internet access, specific services, and computer resources to carry out their jobs.

B. Employees should be trained on the proper use of the Internet.

C. Use the Internet for Census business only on Census-provided hardware and software.

D. Carefully control the use of the Internet to ensure that the Census Bureau is not exposed to the risks of "hackers," the compromise of sensitive data, or embarrassment by inappropriate use.

E. Ensure that Census computers, networks, and data are not accessible to any unprotected computer systems or networks or unauthorized users.

F. Obtain approval from the Chief, Acquisition and Security Division, for special processing requirements involving Internet access to sensitive computer systems, networks, or data.

G. Request activation or termination of the authorized Internet services.

H. Report any knowledge or suspicion of inappropriate activity and unauthorized system intrusions or modifications immediately to the Chief, ADP Security Branch, ASD.

4.8 Census Public Network

The Census public network has made it possible for the general public to access macro Census statistical data extracts. This data would otherwise have taken several days to be received via mail. Several divisions have provided free statistical databases that range from population tables to TIGER maps. In order to maintain the integrity of the Census public network, the following guidelines should be followed.

Guidelines:

A. Never compromise data integrity and security on the public network.

B. Never allow any Title 13 data (*microdata*) to reside on the public network.

C. Restrict user accounts to authorized Census Bureau employees *only*.

D. Apply the existing Census Bureau user account and password security policy.

E. Ensure that network and system administrators implement adequate security monitoring and logging.

F. Prohibit personal business and home pages.

G. Use the public network for official Census business *only*.

4.9 Facsimile Machines

Facsimile (FAX) machines are used extensively by the Census Bureau for transmitting and receiving text and graphics. Facsimile devices communicate over public telephone circuits and transmit and receive data in plaintext. However, software and hardware products are available for encrypting FAX data. When communicating sensitive data with a facsimile machine, implement the following guidelines to reduce the likelihood of disclosure.

Guidelines:

A. Place any facsimile machine in the Census Bureau receiving sensitive data in a secured area. (The goal is to eliminate access by users not having a "need-to-know" for very sensitive data, e.g., business indicators.)

B. Coordinate the use of data encryption equipment or dedicated communications lines with the Telecommunications Office. Plan ahead for their use.

C. Staff areas that contain facsimile machines at all times when the room is open.

D. Verify the telephone number of the facsimile machine receiving the information before transmitting sensitive data.

E. Notify the recipient of the time when sensitive information will be transmitted and agree to have that authorized person present at the destination machine when the material is sent.

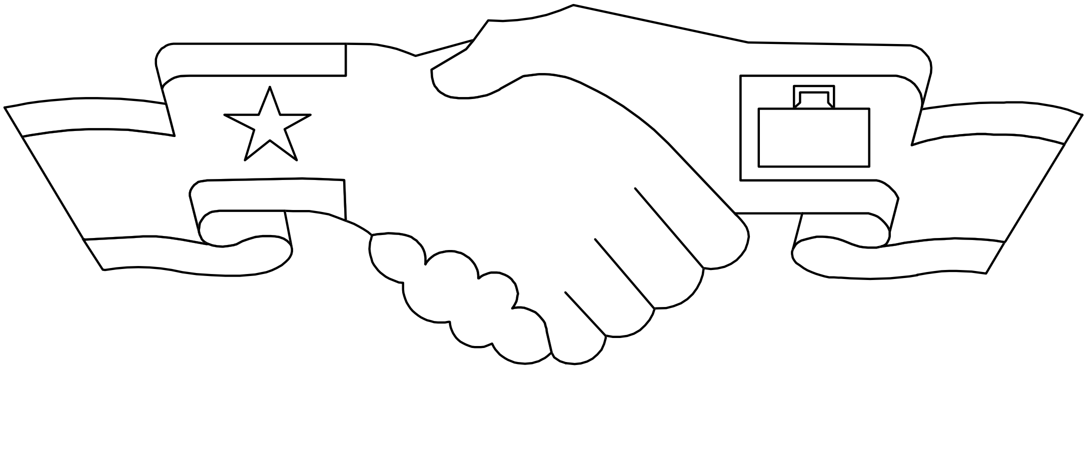
F. ***Never*** send sensitive information to an unattended facsimile machine.

G. Follow appropriate labeling guidelines for faxing Title 13 data (see *Census Administrative Memorandum-General-9*).

H. Distribute facsimile phone numbers only to Census personnel and authorized vendors. This helps eliminate unsolicited documents that can tie up the machine.

PART THREE

Information Technology Security Processing Requirements



CHAPTER 5: SYSTEMS SECURITY PLANNING

5.1 Introduction

The objective of information technology (IT) security planning is to improve protection of information processing resources. System owners and managers must be comfortable that their information and/or processing capabilities are adequately protected from loss, misuse, unauthorized access or modification, unavailability, or undetected activities. The managers must also be assured that all personnel accessing the system, from those performing system management functions to general users, have received security awareness training at levels commensurate with the duties they perform. In addition to training requirements, the IT security planning process (see *Table 5-1*) consists of separate steps that, when combined, will provide management with accurate and reliable documentation of system security.

5.2 System Identification

A system is identified by logical boundaries being drawn around the various processing, communications, storage, and related resources:

(1) They must be under the same direct management control;
(2) With essentially the same function;
(3) Reside in the same environment and;
(4) Have the same characteristics and security needs.

To be defined as a single system, all components need not be physically connected together (e.g., a group of two or more stand-alone personal computers in an office may be identified as a single system if they meet all the criteria above.) Every system identified must be categorized as either a major application system or as a general support system.

A **Major Application System** means an application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. These are systems that perform clearly defined functions for which there are readily identifiable security considerations and needs. Such a system might actually comprise of many individual application programs and hardware, software, and telecommunications components. They can be either a major software application or combination of hardware/software where the only purpose of the system is to support a specific mission-related function (e.g., payroll).

All Federal applications require some level of protection. Certain applications, because of the information in them, require special management oversight and should be treated as major. Adequate security for other applications should be provided by the general support systems in which they operate.

A **General Support System** is an interconnected set of information resources under the same direct management control which shares common functionality. A system normally includes hardware, software, information, data, applications, communications, facilities, and people. Such a system can be, for example, a local area network (LAN) including smart terminals that support a branch office, an agency-wide backbone, a communications network, a departmental data processing center including its operating system and utilities, a tactical radio network, or a shared information processing service organization (ISPO). Normally, the purpose of a general support system is to provide processing or communications support.

Guidelines:

A. Identify any and all systems that are developed, maintained or used by the organization.

B. Categorize each system as either a "Major Application System" or as a "General Support System".

C. Keep an up-to-date inventory of each general support system which includes the corresponding major application system.

D. Notify the ADP Security Branch when new systems are planned or developed and changes are made to existing systems.

5.3 Security Training

Awareness of and training on security responsibilities as well as training in how to fulfill them are an important element in the security of IT systems. Individuals should be well versed in the rules of the system, and the awareness and security training should be consistent with guidance issued by NIST and OPM. Division and office chiefs shall implement the following guidelines.

Guidelines:

A. Formally designate a Division/Local Security Officer (DSO) (see *Appendix 2*) to coordinate security awareness training within the division or office.

B. Make system managers and responsible personnel aware of system security requirements and features through formal and informal training.

C. Perform regular and refresher security awareness training on the Bureau's policies and guidelines for the use of computers (both stand-alone and networked) for all personnel within the division or office.

D. Ensure personnel responsible for system security within the Division or Office are proficient in the initial handling of any security problems that are encountered.

E. Report all IT security-related events to the Chief, ADP Security Branch (see *Section 3.15-Security Incident Reporting*).

5.4 Risk Management/Assessment

Risk is the possibility of something adverse happening. Risk management is the process of assessing risk, taking steps to reduce risk to an acceptable level, and maintaining that level of risk.

Guidelines:

A. By using a risk-based approach, assess system risks and determine security controls needed. This risk assessment approach should consider the value of the system, threats, vulnerabilities, and the effectiveness of current or proposed safeguards.

B. Implement effective safeguards to counter the threats and vulnerabilities identified for each system using the requirements of this document as the minimum standard.

C. Determine whether the residual risks are acceptable and accept system risk prior to placing system into operation.

D. Evaluate the effectiveness of controls through monitoring and annual review.

E. Incorporate additional security measures into software applications whose level of risk requires a greater level of security than an operating system can provide.

F. Conduct a new risk assessment when major changes have been made to the system.

5.5 Establish Security Controls

Organizations are required to establish and document controls implemented to assure adequate security for all information processed, transmitted, or stored in Census Bureau automated information systems. For security to be most effective, the controls must be part of day-to-day operations. This is best accomplished by planning for security, not as a separate activity, but as an integral part of overall planning. Adequate security is "security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information."

Guidelines:

A. Implement cost-effective technical, operational, and management security controls for each identified system to provide for adequate security of IT resources.

B. Prepare a security plan for all general support systems in the organization in accordance with Bureau and Department formats.

C. With the general support system security plan, include a list and description of all application systems that are being protected by the general support system.

D. Prepare a security plan for all major application systems that require additional security controls beyond that of the general support system.

E. Review system security controls, safeguards, and plans at least annually to verify that the information is accurate.

F. Forward security plans and changes to the ADP Security Branch.

5.6 Business Recovery Planning

Organizations should assure that there is an ability to recover and provide service sufficiently to meet the minimal needs of the users of the system in the event of service interruptions.

Guidelines**:**

A. Develop, document, and update a viable business recovery plan (BRP) for each system identified by the organization which should include:

1. A list of critical functions performed.
2. The minimum space and equipment required to restore the organization to minimum operational levels.
3. The time frame that the resource is needed.
4. A list of key personnel and their responsibilities.

B. Designate one responsible individual to coordinate the development, maintenance and testing of the recovery plan.

C. Test the BRP and document the results at least annually.

D. Maintain the BRP in a secure but prominent location such that the plan can be carried out when business recovery is needed. A copy and changes to the plan should be provided to the ADP Security Branch and available for test and inspection.

5.7 Certification, Verification and Accreditation

Certification is a technical evaluation that indicates how well an IT system meets a specified set of security requirements. Following system certification, a formal verification review is conducted to ensure that all security controls identified are current and that the system is operating in the manner described in the security plan. Accreditation is management authorization and approval to process information in an operational environment.

Guidelines:

A. Fully test all identified system security control measures prior to using the system.

B. Ensure that system owners complete certification testing for each system for which they are responsible.

C. Document system certification using the "Abbreviated Certification Methodology Worksheets" provided by the ADP Security Branch.

D. Forward completed certification worksheets to the ADP Security Branch for accreditation.

E. Review completed certifications annually and make changes whenever significant changes are made to existing systems or new systems are developed.

F. Perform monitoring and periodic inspections to ensure proper implementation and effectiveness of security controls and assist the ADP Security Branch with verification reviews.

Table 5.1 ADP Security Planning Process

Census Bureau IT Security Planning Process	
IT Security Planning Activity	**Responsibility**
I. Provide System Identification & Security Plan	**Sponsoring Division**
A. Write a memorandum from sponsoring division chief to Chief, ASD, requesting approval of IT security plan.	
B. Memo should include identification of system components.	
C. Assist with risk assessment (if needed)	
II. Perform Analysis on Planning Documentation	**ADP Security Branch**
A. Ensure minimum security controls are implemented	
B. Assist with risk assessment (if needed)	
C. Ensure risk assessment reveals any additionally needed controls	
D. Inspect processing site (if needed)	
E. Determine accreditation	
F. Write approval memorandum for operational use of system	
III. Certify that Security Controls are Effective	**Sponsoring Division**
A. Test controls to ensure effectiveness	
B. Submit results to ADP Security Branch	
IV. Perform System Accreditation (if needed)	**Senior IRM Official**
A. Authorize as an accredited system	
V. Perform Verification Review	**ADP Security Branch**
A. Perform/coordinate site inspection to evaluate controls	

CHAPTER 6: SPECIAL PROCESSING REQUIREMENTS

6.1 Introduction

The Federal information technology security policies have no exclusionary provisions. They are applicable for information processing systems regardless of whether the sensitive processing services are performed within the Census Bureau, by another Government agency, or by a non-government agency. However, in the latter two situations, the agency is not under the operational management control of Census and must be treated somewhat differently.

6.2 Processing Another Agency's Data

Many Census Bureau programs require the input of data from other Federal Government, state, and non-government organizations. Sometimes these data are protected under the provisions of Federal and state laws or are proprietary in nature and are very sensitive. In any of these cases, Census Bureau employees who process these data must at a minimum protect the data in accordance with policy for protecting Title 13 data. Census Bureau employees must also carefully implement any specific controls required by the sponsoring agency.

Guidelines:

A. Comply with all confidentiality and legal requirements when performing reimbursable work under the agency's data collection authority or when using the agency's records.

B. At a minimum, implement the security controls cited in this document.

C. Unless specifically approved by a written agreement, do not commingle the data provided by the sponsoring agency with Census or other data.

D. Thoroughly inspect procedures for properly handling another agency's data.

6.3 Processing Census Bureau Data by Another Government Agency or Contractor

Census Bureau policy is to take all necessary precautions and safeguards to protect the confidentiality of Census data regardless of storage media (paper, magnetic, electronic, file, etc.) from the time of inception or collection until the information is destroyed. A “contractor” includes other Government agencies; nonprofit associations; educational institutions; private corporations, organizations, or individuals; and other entities with whom processing arrangements are made.

When it is deemed necessary to use contractor personnel to process Title 13 data on other than Census Bureau equipment at a location not under Census Bureau control, the contractor must protect the data while it is in storage, in transit, and in use. The following procedures must be implemented by the division or office before Census data are permitted off-site.

Guidelines:

A. Prepare a memo to the ADP Security Branch requesting approval to use a contractor to process Census data. The memo must include:

   1. Contractor’s company name & address
   2. Point of contact
   3. General description of processing

4. Time frame and duration of processing

B. Ensure that a System Security Plan is completed by the contractor, if off-site processing will last over 30 days.

C. Include the appropriate security-related language (see *Table 6-1*) in any contract, agreement, or other arrangement, formal or informal, with outside contractors.

D. Await an approval memo from the Associate Director for Administration/Controller prior to sending Title 13 data to the contractor.

E. Ensure that contractor personnel are Special Sworn and undergo the appropriate type of investigative processing for suitability and security. The sponsoring division shall submit the names of contractor personnel who need to be Special Sworn to their Administrative Office.

Table 6.1 Security Requirements for Contractor Processing of Census Data

Bureau of the Census Security Requirements for Contractor Processing of Census Data

Policy Statement: The contractor shall implement all Census Bureau IT security policies, standards, and procedures to ensure adequate security of Title 13 data. The appropriate safeguards and controls will be determined and approved by the ADP Security Branch.

Management / Administrative Controls

Special Sworn Status: Contractor personnel having direct access to Title 13 data must have a "need to know" the information in the course of performing their official duties and must become "Special Sworn" by completing Form BC-1759 and taking the Oath of Nondisclosure. This oath must be administered by an authorized Census employee or a Notary Public with the Notary's raised seal on the Form BC-1759. The sponsoring division shall submit the names of contractor personnel who will need to be Special Sworn to their Administrative Office.

Controlled Use of Title 13 Data: The contractor may not use Title 13 data for any purpose other than the intended purpose for which it is supplied.

Site Inspections: The contractor's site may be subject to an inspection by the ADP Security Branch to ensure that adequate IT security is being maintained.

Technical Controls

Individual Accountability: Individual accountability must be accomplished by the contractor by identifying and authenticating users of its system and subsequently tracing actions on the system to the user who initiated them.

Co-processing & Commingling of Title 13 Data: Contractor computer systems used to process Census data must, if possible, be operated only for the processing of Census Bureau data. If Census data is placed upon a shared computer system, controls must be put in place allowing only individuals of Special Sworn Status access. Do not commingle Census Bureau data. The contractor must ensure that Title 13 data cannot be extracted from the computer during processing, such as by a remote terminal or remote access.

Operational Controls

Faxing Title 13 Data: Documents, properly labeled, containing Title 13 data may be faxed to Census Bureau locations only if the fax telephone number is first verified and a

Table 6.1 Security Requirements for Contractor Processing of Census

Bureau of the Census Security Requirements for Contractor Processing of Census Data

Operational Controls (continued)

designated person is at the fax machine to receive the document.

Protected Communications: When transmitting sensitive data external dedicated lines must be used, and/or data must be encrypted.

E-Mail: Transmission of sensitive information by e-mail must be encrypted as an attachment to the mail message.

Protecting Storage Media: The contractor must keep all input and output data secure. Hard copy documents, removable magnetic media, and microform that contain census data must be stored in secured storage containers or a locked room with restricted access.

Acceptable Delivery of Title 13 Data: All Census data must be delivered by delivery services that provide tracing services such as certified mail, priority mail, Federal Express, etc. Multiple packages must be shipped as a unit. Seal and reinforce all packages being sent, enclose a list of the contents being sent, and notify the addressee of the shipment and its contents. The package may only be opened by a "Sworn" employee with the "need-to-know."

Parcels and documents containing sensitive information must be double wrapped. Seal the inner cover, address it, and label it using the appropriate sensitivity designation as described below. The outer cover must be sealed and addressed in the same manner but must not bear the sensitivity label.

Destruction of Title 13 Data: Destroy sensitive material after it has served its intended purpose. Sensitive materials that are too large or numerous to put into burn bags must be kept in a secured area until ready for destruction. The destruction process must prevent recognition or reconstruction of the information.

In most cases, the contractor must return listings containing sensitive Census data to the Census Bureau for disposal. In the case that permission has been granted to the contractor to destroy sensitive material, the following methods must be used:

Recycling - When paper listings containing sensitive data are destroyed through recycling, it is essential that none of the data is restorable from the recycled product. Also, sensitive waste must be carefully controlled by Census employees or contractors with Special Sworn Status until the material is completely destroyed and unrecoverable.

Table 6.1 Security Requirements for Contractor Processing of Census

Bureau of the Census Security Requirements for Contractor Processing of Census Data

Operational Controls (Continued)

Burning - Use EPA-approved public incinerators. When burning sensitive material, examine ash residue if possible. If there are any large pieces of unburned material, reburn it until totally destroyed.

Shredding - Use shredders that reduce residue particle size to 3/16 of an inch or less in width for destruction of sensitive paper and non-paper products. All material will be shredded in such a manner that recognition or reconstruction is impossible by feeding materials into the shredder vertically or diagonally to chop up sentences. Shredded materials can be thrown in the trash and should not be used for other purposes, such as packaging.

Back Up & Recovery - If possible, the contractor should not back up Census data. If Census data is backed up through a contractor's backup system, the tapes, cartridges, or disks should not be sent offsite. Backups should be kept secured as discussed in the Storage section. All backup tapes, cartridges, diskettes, and hard drives must be cleared prior to reuse (*see below*).

Clearing Magnetic Media: Magnetic media (tapes, disks, hard drives) containing sensitive data must be cleared prior to reuse. (This includes returning magnetic media to a vendor for trade-in, servicing or disposal). To clear, overwrite all sensitive data a minimum of three times with a commercial disk utility program. If unable to overwrite, degauss using a commercial degausser.

Proper Labeling: All output (electronic & non-electronic) generated from the system must be properly labeled, under protection of U.S.C. Title 13 as follows:

Non-public use documents and materials not available to the public that contain information protected by Title 13 U.S.C. should be marked in bold type on each page with the phrase "DISCLOSURE PROHIBITED--TITLE 13 U.S.C."

Reports or memoranda of more than one page that contain information protected by Title 13 U.S.C. must contain the following statement on the cover page in bold type: "THIS (report, memorandum) CONTAINS INFORMATION, THE RELEASE OF WHICH IS PROHIBITED BY TITLE 13 U.S.C. AND IS FOR BUREAU OF THE CENSUS OFFICIAL USE ONLY."

Point of Contact: For further information, regarding handling of Census data, contact your Census sponsoring division the Chief, ADP Security Branch on 301-457-2862.

APPENDIX 1

Security Legislation, Regulatory Policy & Guidance

Appendix 1: SECURITY LEGISLATION, REGULATORY POLICY AND GUIDANCE

Legislation	**Provisions**
Title 13, United States Code	Information will not be used for any purpose other than the statistical purposes for which it is supplied. No publications will be made whereby the data furnished by any particular establishment or individual can be identified. Only sworn officers and employees of the Census Bureau are permitted to examine individual reports, and any release of covered data (microdata) is a criminal act punishable by Federal law.
Computer Security Act of 1987 (P.L. 100-35, as amended)	Requires security training, identification of sensitive systems, and the implementation of security plans.
Privacy Act of 1974 (P.L. 93-579, as amended; Title 5, United States Code, Section 552a)	Provides for the protection and accuracy of information about individuals.
Electronic Communications Privacy Act (P.L. 99-508)	Provides for the protection of transmissions by P.L. 99-508 various means of communications technology.
Counterfeit Access Device Act and Computer Fraud and Abuse Act of 1984 (P.L. 98-473) and Computer Fraud and Abuse Act of 1986 (P.L. 99-474; Title 18, United States Code)	Establishes computer-related crime as an offense with specific penalties.
Federal Managers Financial Integrity Act (Public Law 97-225)	Requires the use of internal controls to reduce fraud, waste and abuse.
Title 18, United States Code, Section 1905	Establishes penalties for improper disclosure of trade secrets.
Title 17, United States Code	Protects copyrighted computer software
Paperwork Reduction Act of 1980 (P.L. 96-511, as amended)	Establishes the Federal Information Resources Management (IRM) program.

Policy or Guidance	**Provisions**
Computer Matching and Privacy Protection Act of 1988 (P.L. 100-503, as amended; Title 5, United States Code)	Establishes procedures to ensure the accuracy of computer matching programs.
OMB Circular No. A-130	Assigns Government-wide security responsibilities and describes minimum agency security program components.
OMB Bulletin No. 90-08	Provides detailed guidance for the preparation of security plans.
OMB Circular A-127	Establishes policies and procedures for financial management systems.
OMB Circular No. A-123	Requires the establishment and periodic review of internal controls.
OPM's Federal Personnel Manual (Chapters 731, 732)	Establishes policies on position sensitivity, personnel screening, and security investigations.
NIST's Federal Information Processing Standards (FIPS)	Provides guidelines and establishes mandatory standards criteria on various security issues (e.g., risk analysis, certification, and accreditation)
GSA's Federal Information Resources Management Regulation (FIRMR)	Provides general guidance on privacy and security issues, including acquisition and disposition
OPM's 5 CFR 930	Requires training for all employees involved in the management and use of Federal computer systems that process sensitive information
NIST's Computer Security Training Guidelines	Provides guidance for developing or selecting training in computer security awareness and accepted security knowledge, skills, and abilities.
Tax Information Security Guidelines-- IRS Publication 1075	Provides detailed requirements for using and safeguarding Federal Tax Return Data.

APPENDIX 2

Division/Office Security Officer (DSO) Designation Form

BUREAU OF THE CENSUS DIVISION/OFFICE SECURITY OFFICER DESIGNATION

I. To be completed by Division/Office Chief:

The following person is designated as the DSO:

DIVISION	
NAME	
TITLE	
BRANCH	
TELEPHONE NUMBER	

Signature____ **Date**__________

II. To be completed by DSO:

I have been formally designated as the Division's Security Officer and understand that I am responsible for coordinating security regulations and requirements. This includes:

a. Certifying that security requirements of divisional/office application or general support systems are being or will be met.
b. Ensuring that requests for accreditation of computer systems are completed in accordance with the published procedures.
c. Obtaining protective measures for physical security threats such as deadbolt locks on doors, placement of electrical wiring, etc.
d. Ensuring compliance with all legal requirements concerning the use of commercial proprietary software, e.g., respecting copyrights and obtaining site licenses.
e. Maintaining an inventory of hardware and software within the office/division.
f. Coordinating the development of a division Business Recovery Plan and ensuring that the plans are tested and maintained.
g. Ensuring risk analyses are completed to determine cost-effective and essential safeguards.
h. Ensuring preparation of security plans for sensitive systems.
i. Attending security awareness and related training programs and distributing security awareness information to the office/division when appropriate.
j. Reporting ADP security incidents (including computer viruses) within the division to the ADP Security Branch, Acquisition & Security Division (ASD).
k. Reporting security incidents, other than ADP, to the Security Services Branch, ASD.
l. Act as division/office information contact concerning people in "Special Sworn Status" (SSS).
m. Act as point of contact in the maintenance of the division/office vital records listing.
n. Assist the Security Services Branch, ASD, in informing personnel of badge expiration.
o. Act as Division/Office Safety Officer.
p. Provide input to the Acquisition & Security Division for preparation of reports to higher authorities concerning sensitive and/or national security information systems.

Signature ____ **Date** ________

APPENDIX 3

Glossary & References

Glossary

Accreditation - Management authorization and approval to process sensitive information in an operational environment. Issued by a designated official, it usually includes any constraints for processing in the environment. It is normally based on a certification.

Backbone - A local area network (LAN) that connects all the other LAN segments and provides a medium for conducting Census Bureau data communications.

Certification - The technical evaluation that establishes the extent to which a computer system, application or network design and implementation meet a pre-specified set of security requirements.

Coaxial Cable - Communications cable sometimes used to construct the backbone of a local area network. All transmissions between terminal servers, peripherals and processors are communicated over the coaxial cable.

Encryption - The process of scrambling and unscrambling sensitive data to prevent unauthorized disclosure. Federal government applications that are sensitive must be encrypted. The encryption methodology utilized must conform to the provisions of the Data Encryption Standard (DES). The technical specifications of the DES are found in FIPS PUB-46.

Ethernet - A local area network protocol using a carrier sensing multiple access with collision detection (CSMA/CD) scheme to arbitrate the use of a 10 megabit-per-second baseband coaxial cable.

Fiber Optic - A transmission medium designed to transmit digital signals as pulses of light.

Gateway - A device that interconnects two networks and is required to manage the differences between the networks it connects. It also controls the changing of addressing domains and handles user authorization, usage accounting, and protocol conversion.

Hyperchannel - A very high speed, inter-computer Local Area Network that is capable of exchanging files between similar and dissimilar hosts.

Host - A computer processor primarily devoted to applications processing, but which can also provide services such as down-line loading to a target processor or router.

LAN (Local Area Network) - A data communications system that offers high-speed communications channels optimized for connecting information processing equipment.

Modem - A functional unit that modulates and demodulates signals. One of the functions of a modem is to enable digital signals to be transmitted over analog transmission facilities.

Object - A passive entity that contains or receives information. Access to an object implies access to the information if contains. Examples of objects are: records, blocks, pages, segments, files, directories, directory trees, and programs, as well as bits, bytes, works, fields, processors, video displays, keyboards, clocks, printers, and network nodes.

Object Reuse - The reassignment and reuse of a storage medium (e.g., page frame, disk sector, magnetic tape) that once contained one or more objects.

Plaintext - Computer data that is in readable form and is not scrambled or encrypted.

Public Switched Telephone Network (PSTN) - Telephone system which provides service to analog telephone subscribers. It handles voice communications and data communications via modems and is gradually being converted to a digital network. The network is primarily provided by AT&T and the Bell Operating Companies.

Repeaters - Network devices used to connect two physically separated LAN segments.

Risk - the possibility of harm or loss to any software, data, hardware, administrative, physical, communications, or personnel resource within an automated information system or activity.

Routers - Devices or processors that can send or receive data packets and route them from one process or device to another.

Sensitive Data - Data which is protected from compromise by the Privacy Act, Title 13, the Freedom of Information Act (FOIA), or is designated as such by management. This includes proprietary data, financial data, and data which if improperly disclosed could adversely affect the ability of the Census Bureau to accomplish its mission.

Stand-Alone Personal Computer - A personal computer (PC) that is not configured to a network or capable of interfacing with another PC.

System - A system is identified by logical boundaries being drawn around the various processing communications, storage, and related resources. They must be under the same direct management control (not responsibility), perform essentially the same function, reside in the same environment and have the same characteristics and security needs. A system does not have to be physically connected together.

Threat - An activity, deliberate or unintentional, with the potential for causing harm to an automated information system or activity.

Terminal Server - A device that controls communications between terminals and hosts. Up to eight input/output devices can be configured to the network through a server. These devices can be modems, printers, display terminals, or other peripheral equipment.

Unshielded twisted pair - A local area network that uses two pairs of twisted, unshielded wires to connect a node to a device called a hub. The wiring is similar to that used for telephone sets. The hub can connect several nodes (usually 8 to 12) to the backbone cable. Also referred to as UTP and 10BaseT.

Vulnerability - A flaw or weakness that may allow harm to occur to an automated information system or activity.

References

Census Administrative Manual (CAM) Chapters: S1-*Security Program Administration*, S2-*Risk Management*, S3-*Physical Security*, S4-*Security of Property*, S7-*Contingency Planning and Recovery*, S8-*Personnel Security.*

Census Administrative Manual (CAM) Numbered Memoranda-General: No. 9 - *Guidelines for "Census Confidential" Material*, No. 14 - *Violations of Confidentiality*, No. 16 - *Destruction of Sensitive Material,* No. 19 - *New Building Pass and Investigative Procedures for Contractors and Individuals with Special Sworn Status.*

Fites, P., Kratz, M., *Information Systems Security: A Practitioner's Reference*, 1996.

Department of Commerce, *National Security Information Manual.*

Department of Commerce, *Information Technology Management Handbook*, *Chapter 10: Information Technology Security Manual.*

Department of Commerce, *Guidelines for Developing and Evaluating Security Plans for Sensitive and Classified Systems*, February 1992.

Department of Commerce, *Guidelines for Conducting Information Technology Security Verification Reviews of Sensitive and Classified Systems.*

Guttman, B., Roback, E., NIST Special Publication 800-12: *An Introduction to Computer Security: The NIST Handbook.*

Hutt, A., Bosworth, S., Hoyt, D., *Computer Security Handbook*, Third Edition, 1995.

Office of Management & Budget (OMB) Circular A-130, *Management of Federal Information Resources*, *Appendix III: Security of Federal Automated Information Systems*, February 1996.

OMB Bulletin No. 88-16, *Guidance for Preparation and Submission of Security Plans for Federal Computer Systems Containing Sensitive Information*, July, 1988.

OMB Bulletin No. 90-08, *Guidance for Preparation of Security Plans for Federal Computer Systems that Contain Sensitive Information*, July 1990.

Swanson, M., Guttman, B., NIST Special Publication 800-14: *Generally Accepted Principles and Practices for Securing Information Technology Systems.*