

UNITED STATES
**DEPARTMENT OF
THE TREASURY**



TREASURY INFORMATION TECHNOLOGY SECURITY PROGRAM

TD P 85-01

**VOLUME I
POLICY**

**Part 1
Sensitive Systems**

DOCUMENT CHANGE HISTORY

Version Number	Date	Description
1.0	June 12, 2003	Initial Release

TABLE OF CONTENTS

1. INTRODUCTION.....	1-1
1.1 SECURITY PROGRAM POLICY SCOPE.....	1-1
1.2 AUTHORITIES.....	1-1
1.3 POLICY OVERVIEW.....	1-2
1.4 DOCUMENT ORGANIZATION.....	1-3
2. OVERVIEW.....	2-1
2.1 DEFINITIONS.....	2-1
2.1.1 Availability.....	2-1
2.1.2 Classified Information.....	2-1
2.1.3 Confidentiality.....	2-1
2.1.4 Foreign Intelligence Information.....	2-1
2.1.5 General Support System.....	2-1
2.1.6 Integrity.....	2-2
2.1.7 Information Technology.....	2-2
2.1.8 Major Application.....	2-2
2.1.9 Program.....	2-2
2.1.10 Public Information.....	2-2
2.1.11 Sensitive Information.....	2-3
2.1.12 Treasury System.....	2-3
2.2 THREAT.....	2-3
2.2.1 Internal Threats.....	2-4
2.2.2 Criminal Threats.....	2-4
2.2.3 Foreign Threats.....	2-5
2.3 GENERAL POLICY.....	2-5
2.4 ROLES AND RESPONSIBILITIES.....	2-6
3. MANAGEMENT POLICIES.....	3-1
3.1 CAPITAL PLANNING AND INVESTMENT CONTROL.....	3-1
3.2 CONTRACTORS AND OUTSOURCED OPERATIONS.....	3-1
3.3 PERFORMANCE MEASURES AND METRICS.....	3-1
3.4 CRITICAL INFRASTRUCTURE PROTECTION.....	3-1
3.5 SYSTEM DEVELOPMENT LIFE CYCLE.....	3-2
3.6 SECURITY CHANGE MANAGEMENT.....	3-2
3.7 RISK MANAGEMENT.....	3-2
3.8 CERTIFICATION AND ACCREDITATION.....	3-3
3.8.1 Certification.....	3-3
3.8.2 Accreditation.....	3-3
3.8.3 Certification and Accreditation Process.....	3-4
3.9 IT SECURITY REVIEW AND ASSISTANCE PROGRAM.....	3-4
3.10 SECURITY WORKING GROUPS AND FORUMS.....	3-4
3.10.1 Treasury Information Technology Security Policy Forum.....	3-4
3.10.2 Treasury Infrastructure Protection Panel.....	3-4
3.10.3 Treasury Information Technology Security Training Forum.....	3-5
3.10.4 CIP Working Group.....	3-5

3.10.5 Compliance Working Group.....	3-5
3.11 DISCIPLINARY ACTION.....	3-5
4. OPERATIONAL POLICIES.....	4-1
4.1 PERSONNEL.....	4-1
4.1.1 Background Investigations.....	4-1
4.1.2 Rules of Behavior.....	4-1
4.1.3 Access to Sensitive Information.....	4-1
4.1.4 Separation of Duties.....	4-1
4.1.5 Training and Awareness.....	4-1
4.1.6 Separation From Duty.....	4-2
4.2 IT PHYSICAL SECURITY.....	4-2
4.2.1 General Physical Access.....	4-2
4.2.2 Sensitive Facility.....	4-2
4.3 MEDIA CONTROLS.....	4-3
4.3.1 Media Protection.....	4-3
4.3.2 Media Marking.....	4-3
4.3.3 Sanitization.....	4-3
4.3.4 Production, Input/Output Controls.....	4-3
4.3.5 Disposal.....	4-3
4.4 VOICE COMMUNICATIONS SECURITY.....	4-3
4.4.1 Private Branch Exchange.....	4-3
4.4.2 Telephone Communications.....	4-4
4.4.3 Voice Mail.....	4-4
4.5 DATA COMMUNICATIONS.....	4-4
4.5.1 Telecommunications Protection Techniques.....	4-4
4.5.2 Facsimile.....	4-4
4.5.3 Video Teleconferencing.....	4-4
4.5.4 Voice Over Data Networks.....	4-4
4.6 WIRELESS COMMUNICATIONS.....	4-5
4.6.1 Cellular Phones.....	4-5
4.6.2 Wireless Local Area Network.....	4-5
4.6.3 Pagers.....	4-5
4.6.4 Radio.....	4-5
4.6.5 Multifunctional Wireless Devices.....	4-5
4.7 OVERSEAS COMMUNICATIONS.....	4-6
4.8 EQUIPMENT.....	4-6
4.8.1 Workstations.....	4-6
4.8.2 Laptop Computers.....	4-6
4.8.3 Portable Electronic Devices.....	4-6
4.8.4 Privately Owned Equipment and Software.....	4-6
4.8.5 Hardware and Software Maintenance.....	4-6
4.9 CONVERGING TECHNOLOGIES.....	4-7
4.10 GENERAL IT SECURITY.....	4-7
4.10.1 Security Incident and Violation Handling.....	4-7
4.10.2 Contingency Planning.....	4-7
4.10.3 Documentation (Manuals, Network Diagrams).....	4-8

4.10.4 Information Backup	4-8
5. TECHNICAL POLICIES	5-1
5.1 IDENTIFICATION AND AUTHENTICATION	5-1
5.1.1 Password	5-1
5.2 ACCESS CONTROL	5-1
5.2.1 Automatic Account Lockout	5-1
5.2.2 Automatic Session Lockout	5-1
5.2.3 Warning Banner	5-2
5.3 AUDIT TRAIL	5-2
5.4 NETWORK SECURITY	5-2
5.4.1 Remote Access	5-2
5.4.2 Network Security Monitoring	5-2
5.4.3 Network Connectivity	5-3
5.4.4 Firewalls	5-3
5.4.5 Internet Security	5-3
5.4.6 E-Mail Security	5-3
5.4.7 Privately Owned E-Mail Accounts	5-4
5.4.8 Penetration Testing and Vulnerability Assessment	5-4
5.5 CRYPTOGRAPHY	5-4
5.5.1 Encryption	5-4
5.5.2 Public Key Infrastructure	5-5
5.5.3 Public Key/Private Key	5-5
5.6 VIRUS PROTECTION	5-5
5.7 PRODUCT ASSURANCE	5-6
6. ACRONYMS	6-1

1. INTRODUCTION

The primary purpose of the Department of the Treasury's Information Technology (IT) Security Program is to establish comprehensive, uniform IT security policies to be followed by each bureau in developing its own specific policies and operating directives. The Treasury IT Security Program serves as a foundation for the bureaus to use for their IT security programs. This regulation is binding on all Treasury bureaus and offices.

National policy and standards guide Treasury security policy and requirements. The Treasury IT Security Program clarifies national policies, adapts them to Treasury's specific circumstances, and imposes additional requirements when necessary.

All documents related to the Treasury IT Security Program are living documents. New sections will be developed to keep pace with advances in technology and policy evolution.

TD P 85-01 is issued under the authority of Treasury Directive (TD) 85-01, *Department of the Treasury Information Technology (IT) Security Program*, dated February 13, 2003. TD P 85-01, *Treasury IT Security Program*, supersedes Chapter VI of the existing *Treasury Security Manual*, TD P 71-10, which addresses the areas of telecommunications and information systems security. TD P 71-10, Chapters I–V and Chapters VII and VIII, which address personnel, physical, and information security, emergency preparedness, and domestic counterterrorism, will remain in effect. Bureaus should continue to consult TD P 71-10 for policy in the non-IT security disciplines.

1.1 SECURITY PROGRAM POLICY SCOPE

The Department of the Treasury IT Security Program provides a baseline of IT security policies, standards, and guidelines that apply to the Department of the Treasury bureaus, departmental offices (DO), Office of the Inspector General (OIG), and the Treasury Inspector General for Tax Administration (TIGTA), hereafter referred to collectively as "bureaus." This document outlines policies that relate to management, operational, and technical controls that provide the foundation to ensure confidentiality, integrity, availability, reliability, and nonrepudiation within the Department of the Treasury's IT infrastructure and operations.

The Treasury IT Security Program does not apply to any IT system that processes, stores, or transmits foreign intelligence information under the cognizance of the Special Assistant to the Secretary (National Security) pursuant to Executive Order (E.O.) 12333 or subsequent orders. Contact the Special Assistant to the Secretary (National Security) to obtain security policy and guidance for these systems.

1.2 AUTHORITIES

The Department of the Treasury has established a departmentwide IT security program and organization based on the following Executive orders, public laws, national policy, and Department of the Treasury orders. Volume II, Treasury IT Security Program Handbook, contains additional references.

- a. Public Law 107-347, E-Government Act of 2002, Title III, Federal Information Security Management Act (FISMA) of 2002, December 17, 2002.
- b. Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*.
- c. 26 United States Code (U.S.C.) §6103, Internal Revenue Code.
- d. 41 U.S.C. §423, Procurement Integrity Act.
- e. Public Law 104-106, Clinger-Cohen Act of 1996 [formerly, Information Technology Management Reform Act (ITMRA)], February 10, 1996.
- f. Public Law 93-579, Privacy Act of 1974, as amended. 5 U.S.C. 552a, Washington, DC, July 14, 1987.
- g. E.O. 13231, *Critical Infrastructure Protection in the Information Age*, October 16, 2001, as amended February 28, 2003, Executive orders, amendments of Executive orders, and other laws in connection with the establishment of the Department of Homeland Security.
- h. Presidential Decision Directive (PDD) 63, *Critical Infrastructure Protection*, May 1998.
- i. Title 5 Code of Federal Regulations (CFR) §2635, Office of Government Ethics, *Standards of Ethical Conduct for Employees of the Executive Branch*.
- j. Department of State, 12 Foreign Affairs Manual (FAM) 600, *Information Security Technology*, June 22, 2000.

1.3 POLICY OVERVIEW

A policy delineates the security management structure, assigns responsibilities, and lays the foundation necessary to measure progress and compliance. Policies in this regulation are subdivided under three major control areas: management, operational, and technical.

- a. **Management Controls**—focus on management of the IT security system and the management of system risk. These controls consist of techniques and concerns that management normally addresses.
- b. **Operational Controls**—address security methods focusing on the mechanisms primarily implemented and executed by people. These controls are established to improve the security of a group, a particular system, or a group of systems. These controls require technical or specialized expertise and rely on management and technical controls.
- c. **Technical Controls**—focus on security controls that a computer system executes. These controls can provide automated protection for unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data.

1.4 DOCUMENT ORGANIZATION

TD P 85-01, Treasury Information Technology (IT) Security Program, is divided into two volumes:

- a. Volume I, Treasury IT Security Program Policy
- b. Volume II, Treasury IT Security Program Handbook.

Each volume consists of two parts: Part 1, Sensitive Systems; and Part 2, Classified Systems.

Volume I, Treasury IT Security Program Policy, provides a high-level view of IT security policy for managers and senior executives. IT security practitioners should refer to Volume I for policy information because Volume II will not repeat that information.

Volume II, Treasury IT Security Program Handbook, provides detailed IT security standards and procedures for the IT security practitioner. IT security practitioners should refer to Volume I for the policy.

The structure of Volume I, Treasury IT Security Program Policy, Part 1, Sensitive Systems, is described below:

- Section 1 provides the scope, the authorities, a policy overview, and the organization of the document.
- Section 2 presents an overview of IT security, including basic definitions, threats, general policy, and high-level descriptions of roles and responsibilities.
- Section 3 presents the policies relating to management controls, such as risk management and capital investment planning.
- Section 4 presents the policies relating to operational controls, such as personnel and disaster recovery.
- Section 5 presents the policies relating to technical controls, such as identification and authentication and network security.
- Section 6 provides a list of the acronyms used with this document.

Definitions are provided in Volume II, Treasury IT Security Program Handbook.

2. OVERVIEW

This section provides a short introduction to IT security, providing basic definitions, a discussion on threat, a general policy statement, and high-level descriptions of the roles and responsibilities for positions having IT security responsibilities.

2.1 DEFINITIONS

2.1.1 Availability

Availability is the ability to access a specific resource within a specific time frame as defined with the IT product specification. The availability of an IT system allows the accessibility and usability upon demand by an authorized entity. This state is the prevention of the unauthorized withholding of information or resources.

2.1.2 Classified Information

Information is classified if it has been determined pursuant to E.O. 12958 or any predecessor order or by the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure and is marked to indicate its classified status. Examples include military plans, weapons, or operations; the vulnerabilities or capabilities of systems, installations, projects, or plans relating to national security; foreign government information; foreign relations or foreign activities of the United States; scientific, technological, or economic matters relating to national security; and counternarcotics information when it pertains to foreign relations or national security.

2.1.3 Confidentiality

Confidentiality is defined as the property that information is not made available or disclosed to unauthorized individuals, entities, or processes. Though confidentiality, the unauthorized disclosure of information is prevented.

2.1.4 Foreign Intelligence Information

This type of information relates to the capabilities, intentions, and activities of foreign powers, organizations, or persons, but does not include counterintelligence except for information on international terrorist activities. Contact the Special Assistant to the Secretary (National Security) regarding security policies and procedures relating to IT that processes, stores, or transmits foreign intelligence information.

2.1.5 General Support System

A general support system is an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people. A system can be, for example, a local area network (LAN) including workstations that support a branch office, an agencywide backbone, a communications network, a departmental data processing center and its

operating system and utilities, a tactical radio network, or a shared information processing service organization. (OMB Circular A-130)

2.1.6 Integrity

Integrity is the prevention of the unauthorized modification of information. Integrity is the property that the existence of an object and/or its contents not be destroyed or altered by an unauthorized user. Integrity also means that the contents of an IT system will not be altered to unauthorized values.

2.1.7 Information Technology

The Clinger-Cohen Act defines information technology as any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by an executive agency. For purposes of the preceding definition, “equipment” refers to that used by the Department of the Treasury or by a contractor or another government agency under a contract with the Department of the Treasury if that contractor (a) requires the use of such equipment, or (b) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term “information technology” includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.

2.1.8 Major Application

A major application requires special attention to security because of the potential for risk and the magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Note: All federal applications require some level of protection. Because of the information in them, however, certain applications require special management oversight and should be treated as major. Adequate security for other applications should be provided by the security mechanisms of the systems in which they operate. Examples of major applications include HR Connect, bureau financial systems, or Pay.gov. (OMB Circular A-130)

2.1.9 Program

A program is the process of translating broadly stated mission needs into a set of operational requirements from which specific performance specifications are derived. A program consists of a functional area that supports a Treasury or bureau mission and has associated IT systems and budgetary resources. A program is an organized set of activities directed towards a common purpose, objective, goal, or understanding proposed by a bureau to carry out responsibilities assigned to the organization. Examples of programs include production of U.S. currency, asset forfeiture, and bank supervision.

2.1.10 Public Information

This type of information may be disclosed to the public without restriction but requires protection against erroneous manipulation or alteration. A public Web site is an example.

2.1.11 Sensitive Information

The Computer Security Act of 1987 defines sensitive information as information, the loss, misuse, or unauthorized access to, or modification of which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under 5 U.S.C. Section 552a (the Privacy Act), but that has not been specifically authorized under criteria established by an Executive order or an act of Congress to be kept classified in the interest of national defense or foreign policy. Examples of such sensitive information include personal financial information and information that discloses law enforcement investigative methods. Other particular classes of information may have additional statutory limits on disclosure that require that information to also be treated as sensitive. Examples include tax information, which is protected by Section 6103 of the Internal Revenue Code (26 U.S.C. §6103), and advanced procurement information, protected by the Procurement Integrity Act (41 U.S.C. §423).

The terms “loss,” “misuse,” and “unauthorized access” can involve unauthorized manipulation of data, destruction or loss of data, denial of service, inability to complete or perform a mission, or willful or negligent disclosure of information. The loss, misuse, or unauthorized access of such information could cause damage leading to loss of life or personal injury; loss of property through fraud, theft, or other unlawful means; loss of privacy of an individual; obstruction or impairment of official law enforcement or regulatory functions; gain by an individual, corporation, or any other type of commercial business structure of an unfair advantage in the competitive marketplace; or damage to a person or any type of commercial business structure that has entrusted its proprietary information to the U.S. Government.

2.1.12 Treasury System

A Treasury system is information technology that is a) owned, leased, or operated by a bureau, DO, OIG, TIGTA, or a component thereof; or b) operated by a contractor or another government agency on behalf of a bureau, DO, OIG, TIGTA, or a component thereof.

2.2 THREAT

We live in a highly interconnected world where computers rarely function in a single enclave. Computers are typically connected to the Internet, to all parts of an organization, and to other organizations, both public and private. There is also an increased emphasis within the Federal Government on telecommuting, which requires remote connections to a network, either through dial-in, cable, or digital subscriber line (DSL) connections. In addition, building management services (e.g., badge systems; heating, ventilating, and air conditioning [HVAC]; and entry) may also be connected to the network.

Wireless systems permit personnel to always be in touch with their office, whether by cell phone, pager, or other personal electronic device. Wireless local area networks (WLAN) permit personnel to connect to their network regardless of where they are in their building.

Technologies are also converging. Cell phones now can be used for Internet and e-mail access, for “walkie-talkie” like communications, and even for video. Voice over Internet Protocol (VoIP) permits cost savings by combining voice and data services into one network.

Copiers now also perform network printing, permit printing over the Internet, and provide facsimile (fax) functions.

The increased emphasis on e-Government has provided a new class of government computer user—namely, the general public. Emphasis on achieving a paperless office is moving the sole repository for official records from paper to electronic media.

The threats to Treasury's computer systems have increased as well. The following paragraphs discuss these threats.

2.2.1 Internal Threats

Managers are aware of the usual natural and physical threats to computer systems—earthquakes, tornadoes, fires, floods, electric outages, and plumbing disasters—but do not have the same level of awareness with respect to manmade disasters and threats. Employees tend to be computer literate; most have computers at home. In light of that literacy, the threat from your own employees and/or contractors should not be underestimated. A malicious authorized user can do a lot of damage to Treasury's reputation and to Treasury's data. A careless user can inflict similar damage. Sensitive data, some of it official records, can be lost, corrupted, or compromised through malicious or careless acts. E-mail can be used, either deliberately or without thought, to transmit sensitive data outside your organization to recipients or other computer systems that are not authorized to receive or store the data. A malicious authorized user can also use your computers to attack other computers within Treasury and outside Treasury.

Converging technologies combine the vulnerabilities of each technology and add new ones. Care must be taken to ensure systems are designed with no single points of failure. For example, if you were using VoIP, you would want to ensure that an outage on your data network would not also cause an outage on your voice network (telephone and fax). Similarly, if your building HVAC were connected to your data network, you would want to ensure that an outage or attack on your data network would not also create an outage for your HVAC (and vice versa).

2.2.2 Criminal Threats

Malicious code of all varieties remains a threat to our computer systems. Virus writing tools are available that enable even inexperienced persons to write a virus, and malicious software is becoming much more sophisticated. E-mail software provides capabilities such as scripting, which allows power users to tailor e-mails to the recipient. These capabilities can also be used maliciously to destroy data on your computers and to export malicious code to everyone in the organization's address book. Malicious code can also place back doors into your network that permit access to data or resources on your network.

The hacker community now provides scripts so that even the neophyte can exploit vulnerabilities in your network. Exploits for vulnerabilities in software are often published on the hacker Web sites days after the vulnerability is published. Skilled hackers are targeting e-commerce sites to obtain credit card numbers, which they then sell. Persons with hacking skills are hired by organizations to perform industrial espionage. All they need to do is read or copy a file. They can be in and out of a network without leaving a trace.

Theft of equipment, particularly laptops, is also increasing. Data on a laptop, if not encrypted, can reveal critical information, such as changes to legislation, investigations, or economic analyses. Thefts occur regularly from offices, airports, automobiles, and hotel rooms.

2.2.3 Foreign Threats

Foreign governments conduct espionage not only to protect themselves against perceived threats from the United States but also to obtain information that will be useful to their own industrial base. Terrorists may now have the skills to disrupt Internet communications. Hacker groups with a political agenda have attacked networks of countries they oppose. An example of politically motivated hacking was the hacker war between U.S. hackers and Chinese hackers following our accidental bombing of the Chinese embassy.

Eavesdropping on wireless communications is easy. The equipment for doing so is commercially available. War driving to detect wireless access points is the latest tool used by hackers and spies to obtain access to networks. Employees overseas should assume their cell phone conversations are being monitored.

Software manufacturers are now outsourcing software code development, some of it to foreign countries. Any outsourcing operation raises concerns about the quality of the product produced and invites speculation about whether malicious or criminal code has been inserted into the software. Indeed, it is becoming increasingly difficult to determine the actual source of your IT because the code and equipment are assembled from so many sources.

2.3 GENERAL POLICY

All IT that generates, stores, processes, transfers, or communicates sensitive information shall be protected at a level commensurate with the threat. The level of protection will be determined by the criticality and sensitivity of the information and of the mission supported by the IT, and in compliance with national policy and standards. The threat to U.S. Government and Treasury IT is measured by the capability and intention of the adversary, either foreign or domestic. An adversary may attempt to gain improper access through the exploitation of the vulnerabilities associated with the systems operation to cause harm to the national infrastructure and/or to Treasury missions. The threat shall be identified as foreign, criminal, or other as defined in the glossary in Volume II, Treasury IT Security Program Handbook.

All Treasury major applications and general support systems shall be certified and accredited by an officially designated accrediting authority (DAA). Nonmajor applications shall be certified and accredited as part of the certification and accreditation of the general support system on which the application resides. Certification and accreditation shall be performed before the system is placed into production. Systems shall be reaccredited whenever there is a major change to the system, or every 3 years, whichever occurs first. Systems shall be compliant with minimum security controls as required by federal and departmental security policies, standards, and procedures.

2.4 ROLES AND RESPONSIBILITIES

The executive, technical, and legislative requirements assign responsibilities to divisions, bureaus, and their officials. In high-level terms, this paragraph describes the roles and responsibilities for the Treasury IT Security Program. The Treasury IT Security Program Handbook provides more detailed information on the responsibilities associated with these roles.

- a. The **Secretary of the Treasury** shall—
 - 1) Ensure the integrity, confidentiality, authenticity, availability, and nonrepudiation of information and information systems
 - 2) Ensure the Department of the Treasury practices its information security program throughout the life cycle of each Treasury system
 - 3) Submit annually to the Director of OMB the results of an independent evaluation performed by the agency Inspector General and, for national security systems, an audit of the independent evaluation. This evaluation shall accompany the agency's annual budget submission and should include the results of all annual program reviews by program officials.
- b. **Program officials** are ultimately accountable for the security of programs under their control. They shall determine the acceptable level of risk and adequate level of security. They shall work closely with their Chief Information Officer (CIO) and other officials to ensure a complete understanding of risks, especially the increased risks resulting from interconnecting with other programs and systems over which the program officials have little or no control. This includes determining the appropriate levels of security and periodically testing and evaluating security controls and techniques to ensure that they are cost effective and that they enable, but do not unnecessarily impede, business operations. In consultation with their CIO, program officials shall review each program at least annually.
- c. The **Deputy Assistant Secretary for Information Systems and Chief Information Officer (DASIS/CIO)** is accountable to—
 - 1) Designate a senior agency information security official who will report to the CIO on the implementation and maintenance of the agency information security program and security policies.
 - 2) Participate in developing Treasury performance plans. These plans shall include descriptions of the time periods required to implement the agencywide security program, and the budget, staffing, and training resources necessary to implement the program.
 - 3) Ensure that Treasury security programs integrate fully into Treasury's enterprise architecture and capital planning and investment control processes.
 - 4) Ensure that program officials understand and appropriately address risks, especially the increased risk resulting from interconnecting with other IT and systems over which the program officials have little or no control.
 - 5) Advise the Secretary of the Treasury on IT security matters.

- d. **Bureau heads** shall—
 - 1) Ensure the bureau develops an IT security program in accordance with Treasury policy
 - 2) Ensure the bureau practices its information security program throughout the life cycle of each bureau system
 - 3) Submit a report annually on their IT security program and its annual program reviews to the DASIS/CIO.
- e. The **Bureau CIO** shall manage the sensitive IT security program for the bureau and advise the bureau head on significant issues related to the bureau IT security program.
- f. The **Director, Enterprise IT Security Planning and Assurance (E-ITSPA)**, serves as the departmentwide Information Systems Security Manager (ISSM), the principal advisor on IT security matters. The Director, E-ITSPA, is responsible for issuing departmentwide IT security policy and guidance and for bureau oversight to ensure these policies are implemented.
- g. The **Designated Accrediting Authority (DAA)** is a senior management official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. The DAA is accountable for the risk he or she accepts.
- h. Each bureau shall appoint an **ISSM**. The ISSM shall serve the bureau CIO as the principal advisor on IT security matters. The ISSM is responsible for developing and overseeing the bureau IT security program.
- i. Each program official shall appoint an **Information Systems Security Officer (ISSO)**. The ISSO is the person responsible to the DAA for ensuring the security of an information system throughout its life cycle, from design through disposal.

3. MANAGEMENT POLICIES

3.1 CAPITAL PLANNING AND INVESTMENT CONTROL

Policy: Program officials shall include security requirements in their capital planning and investment business cases. Program officials shall ensure security requirements are adequately funded and documented in accordance with OMB Circular A-11. Treasury and bureau Investment Review Boards shall not approve any capital investment in which the security requirements are not adequately defined and funded.

3.2 CONTRACTORS AND OUTSOURCED OPERATIONS

Policy: All statements of work and contract vehicles shall identify and document the specific security requirements for outsourced services and operations that are required of the contractor. Outsourced services and operations shall adhere to the Department of the Treasury security policies. The security requirements shall include, but not be limited to, how Treasury's sensitive information is to be handled and protected at the contractor's site, including any information stored, processed, or transmitted using the contractor's computer systems; the background investigation and/or clearances required; any security awareness and training required for contractor activities or facilities; and any facility physical security requirements. Contracts must also include disposition instructions for all sensitive Treasury information and IT resources provided during the contract, and procedures for certification that all Treasury information has been purged from any contractor-owned system used to process Treasury information. Bureaus shall conduct reviews to ensure that the security requirements in the contract are implemented and enforced.

3.3 PERFORMANCE MEASURES AND METRICS

Treasury has defined a departmentwide performance measure for the IT security program on certification and accreditation. OMB has issued governmentwide performance measures.

Policy:

- a. Bureaus shall track and provide annual data for their OMB performance measures as defined in OMB reporting guidance for FISMA.
- b. Bureaus shall provide semiannual data on their progress for inclusion in Treasury's performance measure.
- c. Bureaus shall define performance metrics to evaluate the effectiveness of their IT security program.

3.4 CRITICAL INFRASTRUCTURE PROTECTION

Critical infrastructure protection (CIP) is concerned with providing and maintaining adequate levels of security and redundancy to ensure the performance of a minimal set of government and human-related services vital to the protection of people, the stability of the national economy, and the security of the nation. PDD 63, *Critical Infrastructure Protection*, dated May 1998,

stipulates that the national goal is to ensure any interruption or manipulation of these critical national infrastructures is brief, infrequent, manageable, geographically isolated, and minimally detrimental to the welfare of the United States. E.O. 13231, *Critical Infrastructure Protection in the Information Age*, reaffirms the need to continually take actions to secure information systems, emergency preparedness communications, and physical assets.

Policy: DASIS/CIO, in coordination with the bureaus, shall identify and prioritize all IT critical assets in accordance with PDD 63, determine the interdependencies (critical relationships) of these critical assets; develop and implement a Critical Infrastructure Protection Plan to ensure these assets are adequately protected, and ensure vulnerability analysis is conducted on these assets annually.

3.5 SYSTEM DEVELOPMENT LIFE CYCLE

Policy: Bureaus shall ensure that security is integrated into the system development life cycle (SDLC) from the IT system's inception to the system's disposal through adequate and effective management, personnel, operational, and technical control mechanisms.

3.6 SECURITY CHANGE MANAGEMENT

Policy: Bureaus shall prepare configuration management plans for all IT systems and networks. Bureaus shall establish, implement, and enforce change management and configuration management controls on all IT systems and networks. Bureaus shall install security patches in a timely manner in accordance with their configuration management plans.

3.7 RISK MANAGEMENT

Risk management is a process that allows IT managers to balance the operational and economic costs of protective measures to achieve gains in mission capability by protecting the IT systems and data that support their organization's missions.

The head of an organizational unit shall ensure that the organization has the capabilities needed to accomplish its mission. The program officials shall determine the security capabilities that their IT systems must have to provide the desired level of mission support in the face of real-world threats. Most organizations have tight budgets for IT security; therefore, IT security spending shall be reviewed as thoroughly as other management decisions. A well-structured risk management methodology, when used effectively, can help management identify appropriate controls for providing the mission-essential security capabilities.

Policy: Bureaus shall establish a risk management program in accordance with National Institute of Standards and Technology Special Publication (NIST SP) 800-30, *Risk Management Guide for Information Technology Systems*. Bureaus shall conduct risk assessments of major applications and general support systems at least every 3 years.

3.8 CERTIFICATION AND ACCREDITATION

3.8.1 Certification

Certification is the comprehensive testing and evaluation of the technical and nontechnical IT security features, and other safeguards used in support of the accreditation process. Certification establishes the extent to which a particular IT design and implementation meet a specified set of security requirements. Certification primarily addresses software and hardware security safeguards, but also considers procedural, physical, and personnel security measures employed to enforce IT security policy.

Policy: Bureaus shall ensure that all new or major upgrades of existing sensitive IT systems and networks are formally certified through a comprehensive evaluation of the technical and nontechnical security features. The certification, made as part of and in support of the accreditation process, shall determine the extent to which a particular design and an implementation plan meet a specified set of security safeguards. Any modification made to sensitive IT systems or networks or to their physical environment, interfaces, or users, requires a review of the impact on the security of the information processed. Any findings resulting from the review could result in a reaccreditation cycle.

3.8.2 Accreditation

Accreditation is the official management authorization to operate an IT system based on the following:

- a. A particular mode of operation
- b. A prescribed set of security safeguards as defined in the system security plan
- c. A defined threat, with stated vulnerabilities and safeguards
- d. A given operational environment
- e. A stated operational concept
- f. A stated interconnection to other IT
- g. An operational necessity
- h. An acceptable level of risk for which the DAA has formally assumed responsibility.

The DAA accepts security responsibility for the operation of certified IT systems and officially declares that a specified IT system shall adequately protect related information.

Policy: Bureaus shall accredit systems at initial operating capability and every 3 years thereafter, or whenever a major change occurs, whichever occurs first. The DAA may grant an Interim Authority to Operate (IATO) for sensitive systems for a maximum time of 6 months. If the DAA has not officially accredited the system by the end of the 6-month period, the DAA may grant a second and final IATO. At the end of 1 calendar year, the DAA shall request a waiver to operate from the bureau head. This waiver shall be considered a material weakness.

3.8.3 Certification and Accreditation Process

Policy: Bureaus shall use one of the following certification and accreditation processes:

- a. NIST Federal Information Processing Standards Publication (FIPS Pub) 102, *Guidelines for Computer Security Certification and Accreditation*; and SP 800-18, *Guidelines for Developing Security Plans for Information Technology Systems*
- b. National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 1000, *National Information Assurance Certification and Accreditation Process (NIACAP)*.

3.9 IT SECURITY REVIEW AND ASSISTANCE PROGRAM

Policy:

- a. Bureaus shall submit IT security policies to E-ITSPA for review and approval prior to publication.
- b. Bureaus shall establish an IT security review and assistance program within their respective security organizations. Bureaus shall conduct their reviews in accordance with NIST SP 800-26, *Security Self-Assessment Guide for Information Technology Systems*.
- c. E-ITSPA shall conduct review and assistance visits throughout the Department to determine the extent to which the bureau and office programs comply with departmental IT security policy, standards, and procedures.

3.10 SECURITY WORKING GROUPS AND FORUMS

3.10.1 Treasury Information Technology Security Policy Forum

The Treasury Information Technology Security Policy Forum assists E-ITSPA in developing security policies and guidelines for information systems technology, promotes organizational relationships and lines of communications, and serves as a forum for the dissemination of information pertaining to state-of-the-art technologies and methods for securing telecommunications and IT systems.

Policy: Bureaus shall appoint a member to the IT Security Policy Forum who possesses at least a Secret clearance. This individual shall be a Treasury employee. Bureau members shall actively participate in the IT Security Policy Forum.

3.10.2 Treasury Infrastructure Protection Panel

The Treasury Infrastructure Protection Panel (TIPP) is chaired by the Treasury Critical Infrastructure Assurance Officer (CIAO). The panel's membership is composed of critical infrastructure assurance officers, each representing a bureau. The panel meets quarterly and serves as the steering committee for the CIP program.

Policy: Bureau CIAOs shall actively participate in the TIPP to ensure an effective CIP program.

3.10.3 Treasury Information Technology Security Training Forum

The Treasury IT Security Training Forum is established to promote collaboration on IT security training efforts throughout the Department and to share information on bureau-developed training activities, methods, and tools, thereby saving costs and avoiding duplication. E-ITSPA shall facilitate and coordinate regular meetings and provide information on governmentwide IT security training efforts.

Policy: Each bureau shall appoint a representative to the Treasury IT Security Training Forum who is responsible for managing that bureau's IT security training program. Bureau members shall actively participate in the Treasury IT Security Training Forum.

3.10.4 CIP Working Group

The CIP Working Group is chaired by the Treasury Critical Infrastructure Protection Officer (CIPO). It meets quarterly or as required to conduct the activities of the Treasury CIP Program, which may include non-cyber matters. The membership is composed of those bureaus having CIP assets, while non-CIP bureau representation is optional. The bureau representative is titled the Bureau CIP Officer (CIPO). The CIPOs have responsibility for managing the bureau's CIP program and address both cyber and non-cyber matters.

Policy: Bureaus shall appoint a representative to the CIP Working Group who is responsible for managing the bureau's cyber CIP program. Bureau members shall actively participate in the CIP Working Group.

3.10.5 Compliance Working Group

The Compliance Working Group is chaired by the Assistant Director, IT Security Oversight and Compliance. The group meets at least quarterly to coordinate the oversight activities and plans of actions and milestones (POA&M) reporting to the OMB.

Policy: Bureaus shall appoint a representative to the Compliance Working Group who is responsible for managing the bureau's IT security oversight program. Bureau members shall actively participate in the Compliance Working Group.

3.11 DISCIPLINARY ACTION

IT Security Incident. An IT security incident is any event and/or condition that has the potential to affect the security and/or accreditation of an IT system and may result from intentional or unintentional actions.

Examples include unauthorized attempts to gain access to information; introduction of malicious code or viruses into an IT system; installing unapproved modems; opening unauthorized firewall ports; installing unauthorized software or an interconnection that could enable a back door to sensitive IT systems, and loss or theft of computer media; or failure of an IT security function to

perform as designed. For reporting purposes, malicious software incidents include any detection of malicious software, whether detected on magnetic media before the media's entry into an IT system or after infection of the IT system, and any actual execution of malicious software.

IT Security Violation. An IT security violation is an event that may result in disclosure of sensitive information to unauthorized individuals, or that results in unauthorized modification or destruction of system data, loss of computer system processing capability, or loss or theft of any computer system resources.

Policy:

- a. Treasury employees may be subject to disciplinary action for failure to comply with Treasury security policy, whether or not the failure results in criminal prosecution.
- b. Non-Treasury federal employees or Treasury contractors who fail to comply with Treasury security policy are subject to having their access to Treasury IT systems and facilities terminated, whether or not the failure results in criminal prosecution.
- c. Any person who improperly discloses sensitive information is subject to criminal and civil penalties and sanctions under a variety of laws (e.g., Privacy Act, Trade Secrets Act, Bank Secrecy Act).

4. OPERATIONAL POLICIES

4.1 PERSONNEL

4.1.1 Background Investigations

Policy: Bureaus shall designate the position sensitivity level for all in-house or contractor positions that use, develop, or operate IT systems. Bureaus shall ensure the incumbents of these positions have favorably adjudicated background investigations commensurate with the defined sensitivity level. Bureaus shall include adequate funding for background investigations in their budgets.

4.1.2 Rules of Behavior

OMB Circular A-130 requires that all general support systems and major applications have rules of the system, which are termed “rules of behavior.” The rules of behavior relate the use of, security in, and acceptable level of risk for, the system.

Policy: Bureaus shall define rules of behavior for all IT systems. Bureaus shall ensure that users of these systems are given training regarding these rules and the disciplinary actions that may result if they violate those rules.

4.1.3 Access to Sensitive Information

Policy: Program officials shall ensure users of the systems supporting their programs have a validated requirement to access their systems.

4.1.4 Separation of Duties

Policy: Bureaus shall divide and separate duties and responsibilities of critical functions among different individuals so that no individual shall have all necessary authority or systems access, which could result in fraudulent or criminal activity. Separation of duties shall prevent a single individual from being able to disrupt or corrupt a critical security process.

4.1.5 Training and Awareness

Policy: Department of the Treasury personnel, including contractors and task force members who are involved with management, use, or operation of any IT systems that handle sensitive information within or under the supervision of the Department, shall receive periodic training at least annually in security awareness and accepted security practices and system rules of behavior. Department of the Treasury personnel, including contractors and task force members with significant security responsibilities, shall receive specialized training specific to their security responsibilities annually. The level of training shall be commensurate with the individual’s duties and responsibilities and is intended to promote a consistent understanding of the principles and concepts of IT systems security. Bureaus shall have a means to track, by name and position, who has received what training and the costs of the training.

4.1.6 Separation From Duty

Policy: Bureaus shall implement procedures to ensure appropriate system accesses are revoked for employees or contractors who leave the bureau, are reassigned to other duties, or are on extended leave, under disciplinary actions, or for other causes.

4.2 IT PHYSICAL SECURITY

4.2.1 General Physical Access

Policy:

- a. Access to Treasury and bureau buildings and structures housing sensitive IT equipment and data shall be limited to authorized personnel. Controls shall be in place for deterring, detecting, monitoring, restricting, and regulating access to specific areas at all times. Controls shall be based on the level of risk and shall be sufficient to safeguard these assets against possible loss, theft, destruction, accidental damage, hazardous conditions, fire, malicious actions, and natural disasters. The risk should be determined in accordance with federal and departmental security policy.
- b. All visitors shall be escorted and must sign in upon entering the facility and sign out when exiting the facility.

4.2.2 Sensitive Facility

Policy:

- a. Bureaus shall incorporate physical protection measures for all facilities where sensitive information is processed, transmitted, or stored based on the level of risk. The risk shall be determined in accordance with federal and departmental security policy.
- b. Bureaus shall secure any sensitive information not suitable for public dissemination in at least one of the following minimum storage requirements: a locked file cabinet, locked desk drawer, a locked overhead storage receptacle, or a similar locked compartment. Materials can also be stored in a room or area having sufficient physical access control measures to afford adequate protection and prevent unauthorized access by members of the public, visitors, or other persons without a need to know. Examples include a locked room or an area where access is controlled via a cipher lock or card reader.
- c. All visitors shall be escorted and must sign in and out upon entering and leaving data centers, server rooms, or communication closets. Visitor logs shall be maintained on file and available for review for 1 year. Contractors' access shall be limited to those work areas requiring their presence. Records of their ingress and egress shall also be maintained for 1 year. The above access policy includes server rooms at non-Treasury and contractor facilities housing Treasury and bureau IT systems.

4.3 MEDIA CONTROLS

4.3.1 Media Protection

Policy: Bureaus shall ensure all media (e.g., diskettes, external drives, and master copies of software) containing sensitive information, including backup media and removable media, are stored in a secure location when not in use. Bureaus shall ensure backup media are stored offsite in accordance with their contingency plans. All media shall be marked with the appropriate sensitivity level.

4.3.2 Media Marking

Policy: Bureaus shall ensure all media containing sensitive information are appropriately marked with the sensitivity of the information stored on the media.

4.3.3 Sanitization

Policy: Bureaus shall ensure that any sensitive information stored on media to be surplused or returned to the manufacturer shall be purged from the media before disposal. Disposal shall be performed using approved sanitization methods. Bureaus shall maintain records certifying that such sanitization was performed.

4.3.4 Production, Input/Output Controls

Policy: Bureaus shall establish procedures to ensure sensitive information cannot be accessed by unauthorized individuals. These procedures shall address not only the paper and electronic outputs from systems but also the transportation or mailing of sensitive media.

4.3.5 Disposal

Policy: Bureaus shall establish procedures to ensure sensitive information stored on any media is transferred to an authorized individual upon the termination or reassignment of an employee or contractor. Bureaus shall ensure sensitive information is purged from the hard drives of any workstation or server that is returned to the surplus pool of equipment or transferred to another individual. Bureaus shall ensure all media containing sensitive information (e.g., paper, diskettes, and removable disk drives) are purged in such a manner that all sensitive information on that media cannot be recovered by ordinary means. Examples of methods of disposal are crosscut shredders, degaussing, and approved disk-wiping software.

4.4 VOICE COMMUNICATIONS SECURITY

4.4.1 Private Branch Exchange

Policy: Bureaus shall provide adequate physical and IT security for all Treasury-owned private branch exchanges (PBX). (Refer to NIST SP 800-24, *PBX Vulnerability Analysis*, for guidance on detecting and fixing vulnerabilities in PBX systems.)

4.4.2 Telephone Communications

Policy: Bureaus shall establish policy for use of unsecured telephones for discussion of sensitive information. Sensitive voice communications that require secure communications shall be secured using National Security Agency (NSA) or NIST approved security devices.

4.4.3 Voice Mail

Policy: Sensitive information shall not be stored in voice mail. Employees shall not use voice mail for sensitive conversations.

4.5 DATA COMMUNICATIONS

4.5.1 Telecommunications Protection Techniques

Policy: Treasury bureaus shall carefully select the telecommunications protection techniques that meet their security needs consistent with departmental and bureau security policies in the most cost-effective manner.

4.5.2 Facsimile

Policy: Bureaus shall implement and enforce appropriate technical controls for fax technology and systems (including fax machines, servers, gateways, software, and protocols) that transmit and receive sensitive information. Fax communications that require secure communications shall be secured using NSA or NIST approved security devices. Bureaus shall configure fax servers to ensure that incoming lines cannot be used to access the network or any data on the fax server.

4.5.3 Video Teleconferencing

Policy: Bureaus shall implement adequate controls to ensure that only individuals authorized to attend a specific video teleconference shall be able to participate in that videoconference. Bureaus shall ensure appropriate transmission protections are in place commensurate with the highest sensitivity of information to be discussed over the video teleconference. Video teleconferencing equipment and software shall be disabled when not in use.

4.5.4 Voice Over Data Networks

This section applies to VoIP and similar technologies that move voice over digital networks using protocols that may have been originally designed for data networking rather than voice. Such technologies include voice over frame relay, voice over asynchronous transfer mode, and voice over digital subscriber line.

Policy: Bureaus shall design voice over data network implementations with sufficient redundancy to ensure network outages do not result in the loss of both voice and data communications. Bureaus shall ensure appropriate identification and authentication

controls, audit logging, and integrity controls are implemented on every component of their voice over data networks. Bureaus shall ensure that physical access to voice over data network components is restricted to authorized personnel. IP telephones shall have identify and assure (I&A) enabled.

4.6 WIRELESS COMMUNICATIONS

Wireless communications are inherently insecure. Bureaus implementing wireless capabilities need to ensure sensitive information is protected from compromise when being transmitted or stored.

4.6.1 Cellular Phones

Policy: Unsecured cellular phones shall not be used to discuss sensitive information. All bureaus using cellular phones shall protect sensitive communications utilizing NIST or NSA approved algorithms and security devices for all new purchases of cellular equipment after January 2004.

4.6.2 Wireless Local Area Network

Policy: The DAA shall approve the implementation and use of WLANs at a specified risk level. Bureaus shall implement encryption and strong identification and authentication on wireless LANs. Bureaus shall scan monthly for rogue access points on their WLANs.

4.6.3 Pagers

Policy: Pagers shall not be used to transmit sensitive information.

4.6.4 Radio

Policy: All bureaus using radios, whether base stations, mobile or handheld, shall protect sensitive communications utilizing NIST or NSA approved algorithms and security devices for all new purchases of equipment after January 2004.

4.6.5 Multifunctional Wireless Devices

Wireless devices have evolved to be multifunctional. The cell phones, pagers, and radios on the market today can surf the Internet and retrieve e-mail. Cell phones not only can take pictures and transmit them but can also be used to play video games. Most of these functions have no security features.

Policy: Functions that cannot be encrypted using NIST or NSA approved cryptographic modules shall not be used to process, store, or transmit sensitive information. Functions that transmit or receive video, infrared (IF), or radio frequency (RF) signals shall be disabled in areas where sensitive information is discussed. Authentication and encryption shall be implemented for any Treasury data stored on the device.

4.7 OVERSEAS COMMUNICATIONS

Policy: All overseas communications shall occur in accordance with the Department of State, 12 FAM 600, *Information Security Technology*.

4.8 EQUIPMENT

4.8.1 Workstations

Policy: Bureaus shall ensure all workstations are either logged off, locked, or use a password-protected screensaver when unattended. Bureaus shall ensure workstations are adequately protected from theft or tampering.

4.8.2 Laptop Computers

Policy: Sensitive information stored on any laptop computer that may be used outside of Treasury facilities or on travel shall be encrypted using FIPS 140-1 or 140-2 approved encryption. Passwords and smart cards shall not be stored on or with the laptop. Laptop computers in offices shall be secured when unattended via a locking cable, locked office, or locked cabinet or desk. Employees shall obtain the written approval of the DAA before taking a laptop computer overseas.

4.8.3 Portable Electronic Devices

Policy: Privately owned portable electronic devices (PED) shall not be used to process, store, or transmit sensitive Treasury information. The DAA shall approve the use of government-owned PEDs to process, store, or transmit sensitive information. Authentication, data encryption, and transmission encryption shall be implemented to protect sensitive information from compromise. The DAA shall approve the use of add-on devices, such as cameras and recorders. Functions that can record or transmit sensitive information via video, IF, or RF shall be disabled in areas where sensitive information is discussed.

4.8.4 Privately Owned Equipment and Software

Policy: Privately owned equipment and software shall not be used to process, access, or store sensitive information without the written prior approval of the DAA. Privately owned equipment shall not be connected to Treasury equipment without the written prior approval of the DAA.

4.8.5 Hardware and Software Maintenance

Policy: Bureaus shall limit access to system software and hardware to authorized personnel. Bureaus shall test, authorize, and approve all new and revised software and hardware before implementation in accordance with their configuration management plan. Bureaus shall manage systems to reduce vulnerabilities through vulnerability testing, promptly installing patches and eliminating or disabling unnecessary services, if

possible. Maintenance ports shall be disabled and shall be enabled only during maintenance.

4.9 CONVERGING TECHNOLOGIES

Many devices, such as copiers and supervisory control and data acquisitions (SCADA) that formerly did not contain IT now do. In addition, some of these devices may be connected to Treasury data networks. Copiers can be used not only to create copies but also to print and fax.

Policy:

- a. Bureaus shall configure any product connected by cable or wireless to systems containing sensitive information to meet the minimum security requirements in this document, including certification and accreditation.
- b. Bureaus shall enforce limited physical access, identification and authentication, and audit logging for SCADA systems such as HVAC and building access that are critical to the security or safety of a facility but are not connected to Treasury networks. Should these systems also contain sensitive information, certification and accreditation is required.
- c. Bureaus shall enforce media sanitization policy for any stand-alone device, such as a copier that contains a hard drive that at any time processed sensitive information.

4.10 GENERAL IT SECURITY

4.10.1 Security Incident and Violation Handling

Policy:

- a. Bureaus shall establish and maintain a bureau incident response capability.
- b. Bureaus shall report significant computer security incidents to the Department of the Treasury Computer Security Incident Response Center (CSIRC) as soon as possible but no more than 1 hour after detection.
- c. Bureaus shall report minor incidents in a monthly incident report.
- d. Bureaus shall report all planned penetration testing and vulnerability assessments to the Treasury CSIRC.

4.10.2 Contingency Planning

Policy: Bureaus shall develop and maintain detailed business, communications, and IT recovery plans, and the associated recovery capability in the event that normal operations are disrupted. All personnel involved with planning efforts shall be identified and trained in executing the plan and recovery capability. Bureaus shall review plans at least quarterly and perform tests of the recovery capability annually.

4.10.3 Documentation (Manuals, Network Diagrams)

Policy: Bureaus shall ensure security requirements for their IT systems are incorporated in the life-cycle documentation defined in TD P 84-01, *Information Systems Life Cycle Manual*.

4.10.4 Information Backup

Policy: Bureaus shall implement and enforce proper backup procedures for all IT systems and information. Backup procedures shall include off-site storage in accordance with the contingency plan.

5. TECHNICAL POLICIES

The design of IT systems that process, store, or transmit sensitive information shall include, at a minimum, the automated security features discussed in paragraphs 5.1–5.3. Security safeguards shall be in place to ensure each person having access to sensitive IT is individually accountable for his or her actions on the system.

5.1 IDENTIFICATION AND AUTHENTICATION

Policy:

- a. User access shall be controlled and limited based on positive user identification and authentication mechanisms that support the minimum requirements of access control, least privilege, and system integrity.
- b. For IT systems requiring authentication controls, the IT system shall ensure that each user is authenticated before IT system access. The least expensive method for authenticating users is a password system in which authentication is performed each time the password is used. More sophisticated authentication techniques, such as smart cards and biological recognition systems (e.g., retina scanners, handprint, and voice recognition), shall be cost justified through the risk assessment process.

5.1.1 Password

Policy: Bureaus shall enforce strong passwords for authentication to Treasury IT systems. Bureaus shall ensure passwords are unique, difficult to guess, and consist of at least eight characters composed of alphanumeric, upper/lower case, and special characters. Treasury users shall not share passwords. Bureaus shall ensure that passwords are changed at least every 90 days.

5.2 ACCESS CONTROL

Policy: Bureaus shall implement access control measures that shall provide protection from unauthorized alteration, loss, unavailability, or disclosure of information. Access control shall follow the principle of least privilege and separation of duties and shall require that a user use unique identifiers on a system.

5.2.1 Automatic Account Lockout

Policy: Bureaus shall implement and enforce an account lockout policy that limits the number of consecutive failed logon attempts and shall configure systems to lock out a user account after a specified number of failed logon attempts.

5.2.2 Automatic Session Lockout

Policy: Bureaus shall implement and enforce threshold limits for the amount of time a session is inactive before the session timeout feature is invoked.

5.2.3 Warning Banner

Policy:

- a. IT systems internal to the Treasury network shall display Department of Justice approved signon warning banners where technically practical.
- b. IT systems accessible to the public shall provide a security and privacy statement at every entry point.

5.3 AUDIT TRAIL

Policy:

Bureaus shall implement audit trails for all components of sensitive IT systems that can maintain an audit trail.

- a. Audit trails shall be sufficient in detail to facilitate the reconstruction of events if unauthorized activity or a malfunction occurs or is suspected. Audit trails shall be reviewed as specified in the IT system security plan. The audit trail shall contain at least the following information:
 - 1) Identity of each user and device accessing or attempting to access an IT system
 - 2) Time and date of the access and the logoff
 - 3) Activities that might modify, bypass, or negate IT security safeguards
 - 4) Security-relevant actions associated with processing.
- b. Bureaus shall ensure their audit trails are protected from modification, unauthorized access, or destruction.
- c. Bureaus shall ensure that audit trails are recorded and retained in accordance with TD P 80-05, *Records and Information Management Program*.

5.4 NETWORK SECURITY

5.4.1 Remote Access

Policy: Bureaus shall ensure remote access capabilities provide strong identification and authentication and protect sensitive information throughout transmission.

5.4.2 Network Security Monitoring

Policy: Bureaus shall monitor their networks for security events. Bureaus shall report any event that is a security incident to the Treasury CSIRC.

5.4.3 Network Connectivity

Policy:

- a. Bureaus shall ensure appropriate identification and authentication controls, audit trails, and integrity controls are implemented on every network component (e.g., routers, switches, firewalls, IDs).
- b. Interconnections between sensitive IT systems and nonbureau IT systems shall be established through controlled interfaces. The controlled interfaces shall be accredited at the highest security level of information on the network.
- c. Bureaus shall document interconnections with other networks with an interconnection agreement signed by both DAAs. The interconnection agreement shall document the security protections on both systems to ensure only acceptable transactions are permitted.

5.4.4 Firewalls

Policy: Bureaus shall restrict physical access to firewalls to authorized personnel. Bureaus shall implement strong identification and authentication for administration of the firewalls. Bureaus shall encrypt remote maintenance paths to the firewalls. Bureaus shall conduct penetration and vulnerability testing on perimeter firewalls at least quarterly to ensure firewall configuration is correct.

5.4.5 Internet Security

Policy:

- a. Any direct connection of Treasury networks to the Internet or to extranets must occur through firewalls that have been certified and accredited. This also applies to any direct connection between trusted environments.
- b. Firewalls shall be configured to prohibit any Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) service that is not explicitly permitted.
- c. Remote connections shall be centrally managed by each bureau and office to ensure integrity of network security.
- d. For the Department's network, the bureaus must request a waiver for using instant messaging and Internet Relay Chat (IRC) capabilities.

5.4.6 E-Mail Security

Policy: Bureaus shall provide appropriate security for their e-mail systems and transmit e-mail in accordance with NIST SP 800-45.

5.4.7 Privately Owned E-Mail Accounts

Policy: Department of the Treasury employees or contractors shall not transmit sensitive Treasury information to any privately owned e-mail account.

5.4.8 Penetration Testing and Vulnerability Assessment

Policy: Bureaus shall conduct internal vulnerability assessments and/or internal penetration tests on IT systems containing sensitive information at least yearly or when significant changes are made to the IT systems to identify security vulnerabilities.

5.5 CRYPTOGRAPHY

Cryptography is a branch of mathematics based on the transformation of data. Cryptography deals with the transformation of ordinary text (plaintext) into coded form (ciphertext) by encryption and the transformation of ciphertext into plaintext by decryption. Cryptography relies on two basic components: an algorithm (e.g., Advanced Encryption Standard [AES]) and a key. The algorithm is the mathematical function used for encryption or decryption, and the key is the parameter used in the transformation.

There are two basic types of cryptography: secret key systems (also called symmetric systems) and public key systems (also called asymmetric systems). In secret key systems, the same key is used for both encryption and decryption—that is, all parties participating in the communication share a single key. In public key systems, there are two keys: a public key and a private key. The public key used for encryption is different from the private key used for decryption. The two keys are mathematically related, but the private key cannot be determined from the public key.

Refer to NIST SP 800-21, *Guideline for Implementing Cryptography in the Federal Government*, for more in-depth information on cryptography.

5.5.1 Encryption

Encryption is the process of changing plaintext into ciphertext for the purpose of security or privacy.

Policy:

- a. Bureaus shall identify IT systems transmitting sensitive information that may require protection based on a risk assessment. If encryption is required, the following methods are acceptable for encrypting sensitive information:
 - 1) Cryptography modules using triple Data Encryption Standard (DES) or AES algorithms that have been validated under FIPS 140-1 or FIPS 140-2
 - 2) NSA Type 1 or 2 encryption.
- b. All bureaus and offices with sensitive encryption applications under their authority shall develop encryption plans for all IT systems.

5.5.2 Public Key Infrastructure

A public key infrastructure (PKI) is an architecture that provides the means to bind public keys to their owners and helps in the distribution of reliable public keys in large heterogeneous networks. Public keys are bound to their owners by public key certificates. These certificates, which contain information such as the owner's name and the associated public key, are issued by a reliable certification authority (CA).

Policy:

- a. PKI oversight shall be provided at the Department level by a Policy Management Authority (PMA) provided by E-ITSPA.
- b. Treasury shall have a root CA. Any additional CAs within Treasury shall be subordinate to the Treasury root.
- c. CAs shall operate under approved certificate policy and certificate practices statement.
- d. The Treasury root CA shall be able to cross certify with the Federal Bridge. The certificate policies and practices statements of CAs subordinate to the Treasury root must comply with the Federal Bridge certificate policy.
- e. All Treasury subordinate CAs shall undergo a compliance audit.

5.5.3 Public Key/Private Key

A public key/private key pair is generated using the PKI. The user retains the private key. The issuing CA signs the public key, creating a public key certificate. These certificates are used by the PKI to validate a public key. Public key/private keys can be used in a public key cryptographic system to encrypt data. They can also be used to create a digital signature.

A digital signature is an electronic analog of a written signature in that the digital signature can be used in proving to the recipient or a third party that the originator did in fact sign the message. Digital signatures may also be generated for stored data and programs so that the integrity of the data and programs may be verified at any later time. Signature generation makes use of a private key to generate a digital signature. Signature verification makes use of a public key that corresponds to, but is not the same as, the private key. The security of a digital signature system is dependent on maintaining the secrecy of users' private keys.

Policy: The same public/private key pair shall not be used for both encryption and digital signature. Users shall not share their private key. If a user shares his or her private key, the user shall be accountable for all transactions signed with the user's private key. Users shall be responsible for the security of their private key.

5.6 VIRUS PROTECTION

Policy: Bureaus shall implement a defense-in-depth strategy that—

- a. Installs antivirus software at the desktop that is properly configured to check all files, Internet downloads, and e-mail

- b. Installs updates to antivirus software and signature files at the desktop timely and expeditiously without requiring the end user to specifically request the update
- c. Installs security patches to servers and desktops in a timely and expeditious manner.

Bureaus may implement appropriate file/protocol/content filtering to protect their data and networks in accordance with their Internet usage policy.

5.7 PRODUCT ASSURANCE

Policy:

- a. Information assurance (IA) shall be considered as a requirement for all systems used to enter, process, store, display, or transmit sensitive information. IA shall be achieved through the acquisition and appropriate implementation of evaluated or validated commercial off-the-shelf (COTS) IA and IA-enabled IT products. These products shall provide for the availability of systems. The products shall also ensure the integrity and confidentiality of information and the authentication and nonrepudiation of parties in electronic transactions.
- b. *Preference* shall be given to the acquisition of COTS IA and IA-enabled IT products (to be used on systems entering, processing, storing, displaying, or transmitting sensitive information) that have been evaluated and validated, as appropriate, in accordance with the following:
 - 1) The International Common Criteria for Information Security Technology Evaluation Mutual Recognition Agreement
 - 2) The NSA/NIST National Information Assurance Partnership (NIAP) Evaluation and Validation Program
 - 3) The NIST FIPS validation program.
- c. The evaluation and validation of COTS IA and IA-enabled IT products shall be conducted by accredited commercial laboratories or by NIST.
- d. Bureaus shall use only cryptographic modules that have been validated in accordance with FIPS 140-1 or FIPS 140-2.

6. ACRONYMS

AES	Advanced Encryption Standard
ANSI	American National Standards Institute
ASM	Assistant Secretary for Management
ASSET	Automated Security Self-Evaluation Tool
BI	Background Investigation
BIA	Business Impact Analysis
CA	Certification Authority
C&A	Certification and Accreditation
CCB	Change Control Board
CD	Compact Disk
CERT	Computer Emergency Response Team
CFO	Chief Financial Officer
CFR	Code of Federal Regulations
CGI	Common Gateway Interface
CIAO	Critical Infrastructure Assurance Officer
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CIPO	Critical Infrastructure Protection Officer
CIRB	Capital Investment Review Board
CNSS	Committee for National Security Systems
COTS	Commercial Off-the-Shelf
CP	Certificate Policy
CPS	Certification Practice Statement
CRB	Change Review Board
CRT	Cathode Ray Tube
CSIRC	Computer Security Incident Response Capability
DAA	Designated Accrediting Authority
DASIS	Deputy Assistant Secretary for Information Systems
DES	Data Encryption Standard
DMZ	Demilitarized Zone
DO	Departmental Office
DoD	Department of Defense
DOS	Denial of Service
DRAM	Dynamic Random Access Memory
DTS	Diplomatic Telecommunications Service
E-mail	Electronic Mail
E-ITPO	Enterprise IT Planning and Operations
E-ITSPA	Enterprise Information Technology Security Planning and Assurance
EAMS	Enterprise Architecture Management System
EFT	Electronic Funds Transfer
E.O.	Executive Order

EPF	Employee Personnel File
FAM	Foreign Affairs Manual
FBI	Federal Bureau of Investigation
FedCIRC	Federal Computer Incident Response Capability
FEMA	Federal Emergency Management Agency
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act
FTE	Full-Time Equivalent
FTP	File Transfer Protocol
FY	Fiscal Year
GAO	General Accounting Office
GRS	General Records Schedule
GSA	General Services Administration
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HVAC	Heating, Ventilation, and Air-Conditioning
I&A	Identification and Authentication
IA	Information Assurance
IATO	Interim Authority to Operate
ICMP	Internet Control Message Protocol
ID	Identification
IDS	Intrusion Detection Systems
IETF	Internet Engineering Task Force
IF	Infrared
IG	Inspector General
IP	Internet Protocol
IR	Infrared
IRC	Internet Relay Chat
IS	Information System
ISO	International Organization for Standardization
ISSM	Information Systems Security Manager
ISSO	Information Systems Security Officer
IT	Information Technology
ITL	Information Technology Laboratory
ITMRA	Information Technology Management Reform Act
kbps	Kilobits Per Second
KMI	Key Management Infrastructure
LAN	Local Area Network
LOU	Limited Official Use

MBI	Minimum Background Investigation
MGCP	Multimedia Gateway Control Protocol
MOU	Memorandum of Understanding
NARA	National Archives and Records Administration
NCIC	National Criminal Investigation Center
NCS	National Communications Systems
NFS	Network File Systems
NIACAP	National Information Assurance Certification and Accreditation Process
NIAP	National Information Assurance Partnership
NII	National Information Infrastructure
NIPC	National Infrastructure Protection Center
NIS	Network Information System
NIST	National Institute of Standards and Technology
NIST SP	National Institute of Standards and Technology Special Publication
NSA	National Security Agency
NSIRC	National Security Incident Response Center
NSTISSC	National Security Telecommunications and Information Systems Security Committee (renamed CNSS)
NSTISSD	National Security Telecommunications and Information Systems Security Directive
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
OIG	Office of the Inspector General
OMB	Office of Management and Budget
OPF	Official Personnel File
PBX	Private Branch Exchange
PC	Personal Computer
PDD	Presidential Decision Directive
PED	Portable Electronic Device
PKI	Public Key Infrastructure
PMA	Policy Management Authority
POA&M	Plan of Action and Milestones
QA	Quality Assurance
RA	Registration Authority
RAM	Random Access Memory
RF	Radio Frequency
ROM	Read Only Memory
RPC	Remote Procedure Call
SA	System Administrator

SCADA	Supervisory Control and Data Acquisition
SDLC	System Development Life Cycle
SF	Standard Form
SIP	Session Initiation Period
SOW	Statement of Work
SP	Special Publication
SSAA	System Security Authorization Agreement
SSBI	Single Scope Background Investigation
SSP	System Security Plan
TCI	Treasury Critical Infrastructure
TCIPP	Treasury Critical Infrastructure Protection Plan
TCP	Transmission Control Protocol
TD	Treasury Directive
TDP	Treasury Directive Publication
TIGTA	Treasury Inspector General for Tax Administration
TIPP	Treasury Infrastructure Protection Panel
TO	Treasury Order
UDP	User Datagram Protocol
UPS	Uninterruptible Power Supply
URL	Uniform Resource Locator
U.S.C.	United States Code
VoIP	Voice over IP
VPN	Virtual Private Network
WAN	Wide Area Network
WLAN	Wireless Local Area Network
WORM	Write-Once, Read-Many
WWW	World Wide Web