

UNITED STATES  
**DEPARTMENT OF  
THE TREASURY**



# **TREASURY INFORMATION TECHNOLOGY SECURITY PROGRAM**

**TD P 85-01**

**VOLUME I  
POLICY**

**Part 2  
Classified Systems**

## DOCUMENT CHANGE HISTORY

<b>Version Number</b>	<b>Date</b>	<b>Description</b>
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 Classified Information ..... 2-1

2.1.2 Dedicated Mode of Operation..... 2-1

2.1.3 Foreign Intelligence Information ..... 2-1

2.1.4 Information Technology ..... 2-1

2.1.5 Multilevel Mode of Operation ..... 2-2

2.1.6 National Security ..... 2-2

2.1.7 Program..... 2-2

2.1.8 Public Information ..... 2-3

2.1.9 Sensitive Information..... 2-3

2.2 THREAT..... 2-3

2.2.1 Internal Threats ..... 2-4

2.2.2 Criminal Threats ..... 2-5

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 ..... 3-2

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 Working Group ..... 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

<b>4. OPERATIONAL POLICIES.....</b>	<b>4-1</b>
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 Classified 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 Classified 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.....	4-4
4.4 VOICE COMMUNICATIONS SECURITY .....	4-4
4.4.1 Private Branch Exchange.....	4-4
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.....	4-5
4.5.3 Video Teleconferencing.....	4-5
4.5.4 Voice over Data Networks.....	4-5
4.6 WIRELESS COMMUNICATIONS.....	4-5
4.6.1 Cellular Phones/Satellite Phone.....	4-6
4.6.2 Wireless Local Area Network.....	4-6
4.6.3 Pagers.....	4-6
4.6.4 Multifunctional Wireless Devices.....	4-6
4.7 OVERSEAS COMMUNICATIONS.....	4-6
4.8 EQUIPMENT.....	4-6
4.8.1 Security and Marking.....	4-6
4.8.2 Workstations .....	4-7
4.8.3 Laptop Computers.....	4-7
4.8.4 Portable Electronic Devices.....	4-7
4.8.5 Copiers .....	4-7
4.8.6 Privately Owned Equipment and Software.....	4-8
4.8.7 Hardware and Software Maintenance.....	4-8
4.9 CONVERGING TECHNOLOGIES.....	4-8
4.10 SEPARATION OF UNCLASSIFIED AND CLASSIFIED IT SYSTEM .....	4-8
4.11 GENERAL IT SECURITY.....	4-9
4.11.1 Security Incident and Violation Handling .....	4-9
4.11.2 Contingency Planning.....	4-9
4.11.3 Documentation (Manuals, Network Diagrams).....	4-9

4.11.4 Information Backup .....	4-9
<b>5. TECHNICAL POLICIES .....</b>	<b>5-1</b>
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 .....	5-2
5.4.4 Guards and Firewalls .....	5-3
5.4.5 Internet/Intranet Security .....	5-3
5.4.6 E-Mail Security .....	5-3
5.4.7 Privately Owned E-Mail Accounts .....	5-3
5.4.8 Penetration Testing and Vulnerability Assessment .....	5-3
5.5 CRYPTOGRAPHY .....	5-3
5.5.1 Encryption .....	5-4
5.5.2 Public Key Infrastructure .....	5-4
5.5.3 Public Key/Private Key .....	5-4
5.6 COMMUNICATIONS SECURITY .....	5-5
5.6.1 Central Office of Record .....	5-5
5.6.2 COMSEC Accounts .....	5-5
5.6.3 COMSEC Custodians .....	5-6
5.6.4 COMSEC Facilities .....	5-6
5.6.5 COMSEC Accounting .....	5-7
5.6.6 Handling of COMSEC Materials .....	5-8
5.6.7 Reporting COMSEC Incidents .....	5-9
5.6.8 Secure Telephone Equipment for Classified Communications .....	5-9
5.6.9 Use of the EKMS System .....	5-11
5.6.10 Control of Top Secret Keying Material .....	5-12
5.7 TEMPEST REQUIREMENTS .....	5-12
5.8 VIRUS PROTECTION .....	5-12
5.9 PRODUCT ASSURANCE .....	5-12
<b>6. ACRONYMS .....</b>	<b>6-1</b>

## **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 individual 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 E.O.s, 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. Public Law 104-106, Clinger-Cohen Act of 1996 [formerly, Information Technology Management Reform Act (ITMRA)], February 10, 1996.
- d. E.O. 12958, *Classified National Security Information*, as amended April 17, 1995, as amended by E.O. 13292, March 25, 2003.
- e. E.O. 13231, *Critical Infrastructure Protection in the Information Age*, October 16, 2001, as amended February 28, 2003, and E.O.s, amendments of E.O.s, and other laws in connection with the establishment of the Department of Homeland Security.
- f. Presidential Decision Directive (PDD) 63, *Critical Infrastructure Protection*, May 1998.
- g. National Security Directive (NSD) 42, *National Policy for the Security of National Security Telecommunications and Information Systems (U)*, July 5, 1990, Confidential.
- h. 5 Code of Federal Regulations (CFR) §2635, Office of Government Ethics, *Standards of Ethical Conduct for Employees of the Executive Branch*.
- i. Department of State, 12 Foreign Affairs Manual (FAM) 600, *Information Security Technology*, June 22, 2000.
- j. Department of State, 12 FAM 500, *Information Security*, October 1, 1999.
- k. 41 United States Code (U.S.C.) §423, Procurement Integrity Act.

### 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 all system users. 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 2, Classified Systems, is described below:

- Section 1 provides the scope, the authorities, a policy overview, and the document organization.
- 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 within 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 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.

#### **2.1.2 Dedicated Mode of Operation**

A classified IT system is operating in the dedicated mode of operation when each user with direct or indirect access to the system, its peripherals, remote terminals, or remote hosts has a valid personnel security clearance for access to *all* classified information on the system **and** a valid need to know for *all* classified information contained within the system.

#### **2.1.3 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 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.

#### **2.1.4 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.

### 2.1.5 Multilevel Mode of Operation

A classified IT system is operating in the multilevel mode of operation when *some* users with direct or indirect access to the system, its peripherals, remote terminals, or remote hosts *do not* have a valid personnel security clearance for access to *all* classified information on the system **and** all users *have* a valid need to know for *that* classified information to which they are to have access. The need to know is based on approval given to the user by an appropriate authority (e.g., the Designated Accrediting Authority [DAA] or Information Systems Security Officer [ISSO]). Different users may have access to some or all of the classified information processed and/or stored in the system, assuming they have been cleared for such classified information.

Multilevel mode is not routinely authorized for classified IT systems. The Director, Enterprise Information Technology Security Planning and Assurance (E-ITSPA), may make exceptions on a case-by-case basis.

### 2.1.6 National Security

Any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—

- a. the function, operation, or use of which—
  - 1) involves intelligence activities
  - 2) involves cryptologic activities related to national security
  - 3) involves command and control of military forces
  - 4) involves equipment that is an integral part of a weapon or weapons system
  - 5) is critical to the direct fulfillment of military or intelligence missions provided that this definition does not apply to a system that is used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).
- b. is protected at all times by procedures established for information that have been specifically authorized under criteria established by an E.O. or an act of Congress to be kept secret in the interest of national defense or foreign policy.

### 2.1.7 Program

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

### **2.1.8 Public Information**

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

### **2.1.9 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 E.O. or an act of Congress to be kept classified in the interest of national defense or foreign policy. Limited Official Use (LOU) is sensitive information. Examples of sensitive information are personal data, such as social security numbers; trade secrets; individual tax returns; presolicitation procurement documents, such as statements of work (SOW); and law enforcement investigative methods.

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 accessing 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 individual privacy; 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.

### **2.1.10 System-High Mode of Operation**

A classified IT system is operating in the system-high mode of operation when each user with direct or indirect access to the system, its peripherals, remote terminals, or remote hosts has a valid personnel security clearance for access to *all* classified information on the system **and** a valid need-to-know for *some* of the classified information contained within the system. The need-to-know is based on approval given to the user by an appropriate authority (e.g., DAA or ISSO). Different users may have access to some or all the classified information processed and/or stored in the system, assuming they have been cleared for such classified information.

### **2.1.11 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 in which 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.

Classified systems have traditionally been stand-alone systems that were not interconnected with any other systems. However, that is no longer the case. There are increasing requirements to interconnect; however, such interconnection exposes the classified systems to increased threats.

Wireless systems permit personnel always to 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 also 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 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 (e.g., earthquakes, tornadoes, fires, floods, electric outages, and plumbing disasters) but do not have the same level of awareness with respect to more sophisticated 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 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, or the reverse.

### **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. Furthermore, malicious code can 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 laptop computers, is also increasing. Data on a laptop computer, 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 classified 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 classified systems shall be certified and accredited by an official DAA. 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 IT 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. Volume II, 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 effort 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 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 classified 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**, 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** 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**. 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.
- j. The **Central Office of Record (COR)** is responsible for the management and oversight of the communications security (COMSEC) program.

### 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 SOWs 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 classified 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 clearances required; any security awareness and training required for contractor activities or facilities; and any facility physical security requirements. These requirements are stated on DD Form 254 (see TD P 71-10, Chapter IV, for instructions). At the expiration of the contract, SOWs and contract vehicles shall require the return of all classified Treasury information and IT resources provided during the life of the contract. Contracts must also include disposition instructions for all classified 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 assure 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 in the Information Age*, 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 (i.e., 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 that are timely 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 classified 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 meets 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 classified 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 implementation plan meets a specified set of security safeguards. Any modification made to classified IT systems or networks, or to their physical environment, interfaces, or users, shall be reviewed for its impact on the security of the information processed. Any findings identified during the review could result in a reaccreditation cycle. The Director, E-ITSPA, shall certify all systems operating at the Top Secret level.

#### **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 systems
- 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 for systems operating at the Top Secret level is the Special Assistant to the Secretary (National Security). The DAA may grant an Interim Authority to Operate (IATO) for

classified systems for a maximum period 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 Director, E-ITSPA. This waiver shall be considered a material weakness.

### **3.8.3 Certification and Accreditation Process**

**Policy:** Bureaus shall use the National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 1000, *National Information Assurance Certification and Accreditation Process (NIACAP)*, for the certification and accreditation process for classified systems.

## **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 Treasury 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 Working Group**

The Treasury IT Security Policy Working Group 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 Working Group who possesses at least a Secret clearance. This individual shall be a Treasury employee. Bureau members shall actively participate in the IT Security Policy Working Group.

### **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 departmentwide IT security training efforts 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 CIPO. The CIPOs have responsibility for managing the bureau's CIP program and addressing 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 action and milestone (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 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 classified 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, regardless of whether 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, regardless of whether the failure results in criminal prosecution.
- c. Any person who improperly discloses classified information is subject to criminal and civil penalties and sanctions under a variety of laws (e.g., National Security 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 ensure personnel accessing classified systems have the appropriate security clearance and need to know. 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 might result if they violate those rules.

#### 4.1.3 Access to Classified Information

**Policy:** Program officials shall ensure users of the systems supporting their programs have a validated requirement (need to know) and an appropriate security clearance 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 who are involved with management, use, or operation of any IT systems that handle classified information within or under the supervision of the Department, shall receive periodic training at least annually in security awareness and accepted security practices and systems rules of behavior. Department of the Treasury personnel, including contractors, 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 classified IT equipment and data shall be limited to authorized appropriately cleared personnel. Controls shall be in place for deterring, detecting, monitoring, restricting, and regulating access to specific areas at all times. Controls shall be in accordance with E.O. 12958. 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 shall sign in upon entering the facility and sign out when exiting the facility.

### **4.2.2 Classified Facility**

**Policy:**

- a. Facilities, areas, or rooms where classified information is processed, transmitted, or stored shall be secured appropriately in accordance with the Directive on Safeguarding Classified National Security Information for the level of classification the IT system is approved to process. The area or room shall be equipped with locks and security devices to prevent unauthorized and uncleared persons from entering. Classified processing shall not take place in areas that cannot be secured to restrict access. The facility, area, or room must be approved for classified processing (see Volume II, Treasury IT Security Program Handbook).
- b. Access to areas where classified processing occurs shall be restricted to persons having a clearance commensurate with the classification of the information being processed and the level for which the system has been accredited.
- c. Uncleared visitors, contractors, and Treasury employees shall be escorted and shall sign in and out upon entering and leaving the facility. Uncleared visitors, contractors, and Treasury employees shall not be allowed entry into any area when classified processing is taking place. Visitor logs shall be maintained on file and available for review for 1 year. Appropriately cleared 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 shall include server rooms at non-Treasury and contractor facilities housing Treasury and bureau IT systems.

- d. All classified information shall be secured in a General Services Administration (GSA) approved Class V or Class VI safe.

### 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 classified 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 in a location approved for storing classified information at the highest classification level of the information on the backup media. All media shall be marked with the appropriate classification level.

#### 4.3.2 Media Marking

**Policy:** Bureaus shall ensure all media containing classified information are appropriately marked with the classification of the information stored on the media. Printed material shall be automatically marked in the header and footer of each page.

Refer to the Security Classification Guide and the Security Control Guide for additional procedures for marking and handling CIP information.

#### 4.3.3 Sanitization

**Policy:** Bureaus shall ensure that any classified information stored on media to be surplus 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. Equipment used to process classified information that contains any memory components shall be sanitized using National Security Agency (NSA) approved methods as a classified item and shall not be reused on unclassified IT or classified IT at a lower classification level.

#### 4.3.4 Production, Input/Output Controls

**Policy:**

- a. Bureaus shall establish procedures to ensure classified 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 classified media.
- b. Printing of classified information shall occur only on printers approved for classified printing. Printing of classified documents shall occur only when a cleared person

having the need to know is attending the printer to ensure that the documents are under the control of a cleared person.

#### **4.3.5 Disposal**

**Policy:** Bureaus shall establish procedures to ensure classified information stored on any media is transferred to an authorized individual upon the termination or reassignment of an employee or contractor. Bureaus shall ensure classified information is purged from the hard drives of any workstation or server that is returned to the surplus pool for that classified IT system or that is transferred to another individual using that system.

Bureaus shall restrict use of systems used for classified processing to use only after the system has been degaussed. No reuse at lower classification level shall be permitted unless the system has been properly sanitized or has been destroyed. Bureaus shall ensure all media containing classified information (e.g., paper, diskettes, and removable disk drives) are purged in such a manner that all classified information on those media cannot be recovered by ordinary means. Examples of methods of disposal are use of crosscut shredders, degaussing, and approved disk-wiping software. See NSTISSAM COMSEC 1-01 or NSTISSI 4004 Appendix B.

### **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). (See National Telecommunications Security Working Group [NTSWG] Guidelines for Computerized Telephone Systems [CTS], ATSWG Standards 2(a) and 2(b).)

#### **4.4.2 Telephone Communications**

**Policy:** Department of the Treasury unsecured telephones shall not be used to discuss classified national security information. See Section 5.6, Communications Security, for policies on the use of secure telephone equipment. Unsecure phones used in areas where classified discussion may occur shall meet TSG 6 standards (approved telephone equipment is listed in TSG 6 Telephone Security Group approved equipment).

#### **4.4.3 Voice Mail**

**Policy:** Classified information shall not be stored in voice mail.

### **4.5 DATA COMMUNICATIONS**

#### **4.5.1 Telecommunications Protection Techniques**

**Policy:** Bureaus shall use NSA-approved type 1 cryptographic devices on circuits used for the transmission of classified information.

#### 4.5.2 Facsimile

**Policy:**

- a. Fax machines used for the transmission or reproduction of classified information shall be approved for use with classified information by a qualified security person. Fax machines used for classified purposes shall be approved by the NSA for that purpose. Faxes used for classified or sensitive information shall be equipped with NSA-approved security devices keyed to the level of information being transmitted by the fax machine.
- b. Fax machines used for the transmission or reproduction of classified information shall be used only in an area approved for classified processing that has controlled access. Uncleared employees, visitors, and contractors shall not have unaccompanied access to the areas used for the operation of fax machines approved for classified information.
- c. Fax machines used for classified information shall not be able to operate in the unattended mode.
- d. The key, cards, or other security devices used with classified fax machines shall be inserted or activated only when the fax machine is attended by a properly cleared person.
- e. Every fax machine approved for use shall have a GSA-approved Class V or Class VI storage container(s) associated with it for the storage of classified information.

#### 4.5.3 Video Teleconferencing

**Policy:** Bureaus shall implement adequate controls to ensure that only individuals with the appropriate clearance and need to know shall be able to participate in the videoconference. Bureaus shall ensure that appropriate transmission protections are in place commensurate with the highest classification 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 not use VoIP technology for any classified data or voice communications.

#### 4.6 WIRELESS COMMUNICATIONS

Wireless communications are inherently insecure. Bureaus implementing wireless capabilities need to ensure that the transmission and storage of classified information is protected from compromise using NSA Type 1 encryption algorithms and encryption devices.

#### 4.6.1 Cellular Phones/Satellite Phone

**Policy:** Only NSA-approved secure cellular phones and secure satellite phones shall be used to discuss classified information. Personnel shall exercise care when using these cellular phones to ensure their conversations are not overheard by persons without the appropriate clearance and need to know. Secure cell or satellite phones shall not be left unattended when not in use. In the United States, these phones shall be secured in a locked car, briefcase, or Class V or Class VI security container when not in use.

NSA-approved secure cell phones shall be used only in countries approved for their use. The Department of State must be consulted before using NSA-approved secure cell phones overseas. Secure cell phones shall not be left unattended and must be secured at a U.S. embassy or with other cleared persons when not in use.

#### 4.6.2 Wireless Local Area Network

**Policy:** Bureaus shall not use WLANs to process, store, or transmit classified information.

#### 4.6.3 Pagers

**Policy:** Pagers shall not be used to transmit classified information.

#### 4.6.4 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:** Only NSA-approved multifunctional devices shall be used to process, transmit, or store classified information. The DAA must approve their use in Treasury.

### 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 Security and Marking

**Policy:** All equipment used to process, transmit, store, copy, or print classified information shall be housed in rooms or areas approved for classified processing at the classification level of the information processed. All equipment shall be marked clearly with the classification level of the information processed.

#### 4.8.2 Workstations

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

#### 4.8.3 Laptop Computers

**Policy:** Classified information stored on any laptop computer that may be used outside of Treasury facilities or on travel shall be encrypted using NSA type I or type II approved encryption. Passwords and smart cards shall not be stored on or with the laptop computer. Laptop computers unattended in offices shall be secured in a safe.

#### 4.8.4 Portable Electronic Devices

**Policy:** Privately owned portable electronic devices (PED) shall not be used to process, store, or transmit classified Treasury information. The DAA shall approve the use of government-owned, NSA-approved PEDs to process, store, or transmit classified information. Authentication, data encryption, and transmission encryption shall be implemented to protect classified information from compromise. Add-on devices, such as cameras and recorders, are prohibited. Privately owned PEDs and government-owned PEDs used to process sensitive information shall not be permitted in conference rooms or secure facilities where classified information is discussed.

#### 4.8.5 Copiers

**Policy:**

- a. Classified information shall be reproduced only on copying machines previously approved by a qualified security person for the reproduction of classified information. Copying machines that contain a hard drive that retains images of copies or that are equipped with a remote maintenance capability shall not be used for the reproduction of classified information if those machines are connected to any network.
- b. Copying machines approved for the reproduction of classified information shall be located in areas where access can be controlled when copying is being performed. These copying machines shall be located in areas that are inaccessible to the public or uncleared persons. These machines shall be installed in a lockable room equipped with a high-security lock that is not keyed to the building master key system and shall be located where access is controlled.
- c. Maintenance shall be performed on copiers approved for classified reproduction only while a properly cleared person escorts the maintenance technician. Memory components shall not leave the facility if found to be inoperable or needing repair. They shall be replaced, and the old component shall be destroyed as classified waste. Toner cartridges shall be inspected for any image retention before being discarded.

#### 4.8.6 Privately Owned Equipment and Software

**Policy:** Privately owned equipment and software shall not be used to process, access, or store classified information. Privately owned equipment shall not be connected to classified Treasury equipment.

#### 4.8.7 Hardware and Software Maintenance

**Policy:** Personnel cleared to at least the classification level of the IT system shall perform all maintenance of equipment and transmission circuits used for classified IT systems. If cleared maintenance personnel are not available, a cleared government person with sufficient technical knowledge to enable the detection of unauthorized alteration or modification to the network shall escort the maintenance 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.

### 4.9 CONVERGING TECHNOLOGIES

Many devices, such as copiers and 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:** Bureaus shall configure any product connected by cable or wireless to systems containing classified information to meet the minimum security requirements in this document, including certification and accreditation. 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 classified information.

### 4.10 SEPARATION OF UNCLASSIFIED AND CLASSIFIED IT SYSTEM

**Policy:**

- a. Classified networks shall not be installed in communications closets and data centers used for unclassified networks unless the area is controlled by cleared personnel. Classified networks and their associated communications circuits shall be isolated from unclassified networks. This policy may be waived by the DAA if a separate access-controlled area or room is built and alarmed to prevent access by uncleared persons, or if all persons with access to the areas are cleared to the level of the classified network.
- b. Classified processors and circuits shall be separated by a minimum distance of one-half meter from unclassified processors or communication circuits and switching equipment. This minimum distance applies to data centers, communications closets, and user workspaces. Specific separation requirements can be found in NSTISSAM/2-95, *Red Black Installation Guidance*. For further guidance, contact the Treasury Certified Tempest Testing Authority.

- c. Information systems approved for classified processing and their peripherals shall not be connected to any system not approved for classified operation. Systems approved for classified processing shall not share peripherals with unclassified processing equipment except through NSA-approved switching devices. Approval for the use of switching devices shall be included in the accreditation documentation.

## **4.11 GENERAL IT SECURITY**

### **4.11.1 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. The Treasury CSIRC shall immediately report any incident occurring on a classified system to the Director, E-ITSPA.

### **4.11.2 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.

### **4.11.3 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*.

### **4.11.4 Information Backup**

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

## 5. TECHNICAL POLICIES

The design of IT systems that process, store, or transmit classified 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 classified information technology is appropriately cleared, has a need to know, and 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:** Classified systems shall display Department of Justice approved sign-on warning banners where technically practical.

## 5.3 AUDIT TRAIL

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

**Policy:**

- 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 classified 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 (i.e., routers, switches, firewalls, IDs).

- b. Interconnections between classified IT systems and nonbureau classified 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 Guards and Firewalls**

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

#### **5.4.5 Internet/Intranet Security**

**Policy:**

- a. Bureaus shall not connect classified systems to the public Internet or to any system that is connected to the public Internet.
- b. The Director, E-ITSPA, must approve the design and implementation of any classified Intranet.

#### **5.4.6 E-Mail Security**

**Policy:** Bureaus shall provide appropriate security for their e-mail systems and 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 classified 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 classified 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 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. All bureaus shall implement NSA Type I or approved Type II endorsed encryption when electronically communicating classified or unclassified national security information.
- b. All bureaus and offices with classified 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 a 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:** Bureaus shall contact E-ITSPA concerning any requirement for a public key infrastructure for classified systems. The Director, E-ITSPA, shall then coordinate these requirements with NSA.

### 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 to 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 also can 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 COMMUNICATIONS SECURITY**

### **5.6.1 Central Office of Record**

**Policy:** The Treasury COR is responsible for policy and operation of all forms of secure communications in all Treasury offices and bureaus. The Treasury COR reports to the Director, E-ITSPA.

### **5.6.2 COMSEC Accounts**

#### **5.6.2.1 Establishment of COMSEC Accounts**

**Policy:** Bureaus shall establish COMSEC accounts through the Treasury COR.

Requirements for COMSEC may be found in Volume II, Treasury IT Security Program Handbook.

#### **5.6.2.2 Closing a COMSEC Account**

**Policy:** When a COMSEC account is no longer needed, the Treasury COR shall be notified. The Treasury COR shall send an inventory of the account for verification by the COMSEC Custodian. After the items in the account have been verified, the Treasury COR shall provide disposition instructions for all key and equipment. After final disposition has been completed, the records of the account shall be audited and the records transferred to the Treasury COR for storage.

#### **5.6.2.3 Termination of a COMSEC Account**

**Policy:** Treasury and bureau COMSEC accounts may be closed by the Department of the Treasury DASIS/CIO at the recommendation of the Treasury COR if two or more consecutive COMSEC audits show that the account is mismanaged or that management has not taken adequate steps to correct serious problems in the account. Accounts may also be closed if frequent COMSEC incidents have occurred that demonstrate a lack of supervision and training of hand-receipt holders by COMSEC personnel.

### 5.6.3 COMSEC Custodians

#### 5.6.3.1 Appointment of Bureau COMSEC Custodians

**Policy:** Bureaus shall appoint in writing (using memorandum format) sufficient COMSEC Custodians and Alternate COMSEC Custodians to support the volume of work their account processes. Appointments shall be signed by a person at the Division Chief level or above by a person in the supervision chain of the custodian. The duty of COMSEC Custodian shall be the primary function of the person appointed to be COMSEC Custodian. Specific selection requirements are found in the Volume II, Treasury IT Security Program Handbook. Appointments shall be forwarded to the Treasury COR.

#### 5.6.3.2 Indoctrination of the Bureau COMSEC Custodians and Alternates

**Policy:** Upon establishment of a new account or appointment of new COMSEC custodians and alternates, these persons shall report to the Treasury COR for cryptographic access and COMSEC briefing by the COR.

#### 5.6.3.3 Temporary Absence of the COMSEC Custodian

**Policy:** If the COMSEC Custodian is away for fewer than 30 days, the alternate custodian shall assume the responsibilities of the COMSEC Custodian. Upon the return of the COMSEC Custodian, the alternate shall inform the custodian of any changes made to the account while the custodian was away. If the COMSEC Custodian is to be absent for more than 30 days, a new COMSEC Custodian must be appointed and the account transferred to the new custodian.

#### 5.6.3.4 Sudden Permanent Departure or Unauthorized Absence of the COMSEC Custodian

**Policy:** Under emergency circumstances, such as the sudden indefinite or permanent departure of the COMSEC Custodian, action shall be taken to appoint a new COMSEC Custodian immediately. If the outgoing custodian is not available to perform a change of custody inventory, the new custodian and an appropriately cleared witness selected by the Division Chief shall perform a complete physical inventory of all items in the COMSEC account. The Treasury COR shall be notified so an inventory may be provided and appropriate actions are taken to safeguard the account. See Volume II, Treasury IT Security Program Handbook, for specifics.

### 5.6.4 COMSEC Facilities

**Policy:** Bureau COMSEC facilities shall be built in accordance with the standards outlined in NSTISSI 4005, *Safeguarding Communications Security (COMSEC) Facilities and Materials*, and its successor standards.

## 5.6.5 COMSEC Accounting

### 5.6.5.1 COMSEC Accounting Methods

**Policy:** COMSEC Accounting shall be performed either manually in accordance with NSTISSC 4005 or electronically using Defense Automatic Integrated System (DAIS) software or through the use of Electronic Key Management System (EKMS).

### 5.6.5.2 COMSEC Material Accounting

**Policy:** Forms used for the control of accountable COMSEC material shall be limited to the Standard Form (SF) 153, L 6061 cards, and those forms electronically generated by DIAS and the Local Management Device (LMD) software of the EKMS system. Paper copies of electronic forms shall be printed and filed as backups for all transactions. This policy shall not apply to transactions made through a data transfer device (DTD). Electronic transactions made through a DTD shall be reconciled to the LMD at least weekly. A hard copy of the DTD transaction shall be prepared and filed each week.

### 5.6.5.3 COMSEC Hand Receipts

**Policy:** All items of COMSEC equipment and keying material shall be hand receipted to the properly cleared user using an SF 153 or L 6061 card. Hand receipts shall be updated annually if the holder is more than 25 miles from the COMSEC Custodian's office. Hand receipts for equipment and keying material issued to users fewer than 25 miles from the custodian's office where the custodian periodically interacts with the account shall be updated periodically but at least every 3 years. Hand receipts for COMSEC equipment and key for emergency contingency locations may be hand receipted to a person who is properly cleared and responsible for maintaining the emergency site.

### 5.6.5.4 COMSEC Files

**Policy:** COMSEC accounting files shall be established by each COMSEC Custodian in either electronic or paper form. A transaction log that records all COMSEC transactions shall be maintained. See Volume II, Treasury IT Security Program Handbook, for contents of COMSEC files.

### 5.6.5.5 Classification of COMSEC Accounting Forms

**Policy:** All COMSEC accounting forms shall be unclassified and marked as "Official Use Only" in accordance with NSA guidelines.

### 5.6.5.6 Transfer of COMSEC Material

**Policy:** COMSEC material shall be transferred only through the COMSEC Custodian. Hand receipt holders shall not move COMSEC material in their possession to other locations without informing the COMSEC Custodian.

### **5.6.5.7 Inventory of COMSEC Material**

**Policy:** Inventories of COMSEC material under the control of bureau COMSEC Custodians shall be made annually. Inventories shall be provided by the Treasury COR to each COMSEC Custodian for verification of all accounting legend code (ALC) 1, 2, 6, and 7 items on hand in each account. Inventories shall be completed and returned to the Treasury COR within 30 days of the date of the inventory. Items not on hand receipt shall be physically inventoried, and the hand receipt shall serve as verification of the presence of items issued to users.

### **5.6.5.8 COMSEC Records**

**Policy:** All COMSEC records shall be kept on file for a minimum of 3 years. Records of incoming COMSEC material shall be maintained until the item is transferred or destroyed.

### **5.6.5.9 Audits of COMSEC Accounts by the Treasury COR**

**Policy:** Audits of bureau COMSEC accounts shall be performed annually by the Treasury COR. Thirty days advance notice of the inventory shall be given, and a copy of the COR's inventory record for the account shall be provided to the custodian to help prepare for the audit. Specific items to be included in the audit are detailed in Volume II, Treasury IT Security Program Handbook.

## **5.6.6 Handling of COMSEC Materials**

### **5.6.6.1 Receipt of COMSEC Material**

**Policy:** All packages of COMSEC Material (Registered Mail or Defense Courier Service [DCS]) shall be opened and inventoried immediately upon receipt by the COMSEC Custodian or an alternate. See Volume II, Treasury IT Security Program Handbook, for proper methodology for examination and discrepancy reporting.

### **5.6.6.2 Storage of COMSEC Material**

**Policy:** Classified COMSEC equipment shall be stored in the manner prescribed for other classified material in accordance with E.O. 12958. COMSEC equipment marked controlled cryptographic items (CCI) shall be stored with double barrier protection in an alarmed room or GSA-approved Class V or VI container. Access to stored COMSEC material is restricted to COMSEC personnel and users.

### **5.6.6.3 Destruction of COMSEC Material**

**Policy:** COMSEC material other than equipment shall be destroyed when no longer required by the bureaus. Detailed instructions on how to destroy COMSEC material can be found in Volume II, Treasury IT Security Program Handbook. An SF 153 shall be prepared by the custodian documenting each item destroyed. Destructions shall be witnessed by a properly cleared individual.

#### 5.6.6.4 Disposition of COMSEC Equipment

**Policy:** The Treasury COR shall be contacted for disposition instructions for all COMSEC equipment considered to exceed a bureau's needs. The Treasury COR shall query each bureau to determine whether the excess COMSEC equipment may be used by other Treasury bureaus.

#### 5.6.7 Reporting COMSEC Incidents

**Policy:** Incidents involving the loss, compromise, or inadvertent destruction or possible compromise or inadvertent destruction of COMSEC equipment or keys shall be reported within 24 hours to the Treasury COR and the NSA. Specific instructions are provided in Volume II, Treasury IT Security Program Handbook.

#### 5.6.8 Secure Telephone Equipment for Classified Communications

The Treasury Department uses several types of security devices to protect classified and sensitive telephone communications. These devices include Secure Telephone Equipment (STE); Secure Telephone Units (STU); and the Future Narrowband Digital Telephones (FNBDT) security units, OMNI and Omega. For simplicity, all these devices are referred to as STEs in the policies below.

##### 5.6.8.1 Security of Keys (Crypto Ignition Keys), Cards, and PINs

**Policy:** FORTEZZA cards, smart cards, and personal identification numbers (PIN) (i.e., keys) that activate the security inherent in the STEs shall not be stored or left installed and active in any security device when unattended. Keys, FORTEZZA cards, smart cards, and PINs that activate the security circuits of these devices shall be stored in a locked cabinet or drawer that is inaccessible to persons who do not have a need to know or do not hold the level of clearance to which the device is keyed.

##### 5.6.8.2 Transport of STE and PIN Numbers Keys

**Policy:** Keys, FORTEZZA cards, smart cards, and PINs shall not be installed when the devices are shipped or transported. When STE equipment is shipped, the keys shall be sent separately in a different container and shipment. STEs may be configured for use before shipment.

##### 5.6.8.3 Transport of STEs

**Policy:** STEs shall be hand carried, shipped registered mail through the U.S. Postal Service (USPS), Federal Express, or the DCS. A signed return receipt is required, along with a signed SF 153 accounting for the device.

##### 5.6.8.4 Use of STEs

**Policy:** STEs shall be used only in offices or rooms in which secure conversations will not be overheard by persons not having a need to know or a proper personal clearance

level. Doors shall be closed when the STE is used in the secure mode of operation. Rooms shall meet 45 Sound Transmission Class (STC) acoustical standards to use speaker phones associated with these devices. Rooms where STEs are installed must be able to be locked and the key controlled by a properly cleared person.

#### **5.6.8.5 Use of STEs for Securing Fax Machines**

**Policy:** STEs used for securing faxes shall be used only in offices or rooms where the security of the equipment can be guaranteed. Rooms where STEs are installed shall be accessible only to persons having the minimum personal clearance to which the device is keyed (e.g., Secret). These fax machines shall not operate in an unattended mode unless a properly cleared person is present and unless the room in which it is installed is approved for open storage at the level to which the STE is keyed. All areas with a secure fax machine shall have a GSA-approved Class V or Class VI storage container available for storing items received over the classified fax machine. Secure fax machines shall not be authorized for a private residence. A memorandum of understanding (MOU) is required for use of a secure fax between the Special Assistant Secretary for National Security and the user's office. The MOU must clearly define the use of the secure fax machine.

#### **5.6.8.6 Use of Secure Cellular and Satellite Phones**

**Policy:** Secure cellular and satellite phones shall be used only in the secure mode in which conversations cannot be overheard by persons who are uncleared or do not have a need to know. Secure cellular and satellite phones shall not be used in public places.

#### **5.6.8.7 Storage and Transport of Secure Cellular and Satellite Phones and Keying Material**

**Policy:**

- a. When not in use, secure cellular and satellite phones shall be kept on the person of the user or locked in a secure place (e.g., safe deposit box, car trunk, or brief case).
- b. Secure cellular and satellite phones shall not be transported in checked baggage or left unattended in carry-on luggage. Keys to activate the devices shall be neither stored nor transported in the same manner as the device.

#### **5.6.8.8 Use of Secure Phones in Residences**

**Policy:** STEs and secure cellular and satellite phones shall be used in private residences if approved in advance by the Treasury COR. Residences shall have a security review, completed by qualified security personnel approved to perform such surveys before the installation of any secure telephone to ensure that the device is properly protected and it can be used securely. Secure phones in residences shall be keyed only to the Secret level unless approval of the Director, E-ITSPA, and the Special Assistant to the Secretary (National Security) is obtained. Rules for installation and use of secure phones in a residence are outlined in the Volume II, Treasury IT Security Program Handbook.

## **5.6.9 Use of the EKMS System**

### **5.6.9.1 Requests for EKMS Credentials**

**Policy:** All requests for EKMS credentials shall be forwarded through the Treasury COR to NSA for processing.

### **5.6.9.2 Security and Use of Local Management Device/Key Processor**

**Policy:**

- a. LMD/KPs shall be used only in areas meeting NSTISSC 4005 security requirements or Director of Central Intelligence Directive (DCID) 1/21 requirements when producing or storing Special Compartmented Information (SCI) key.
- b. Access to the equipment shall be restricted to trained operators and COMSEC personnel.
- c. When not in use, the KP shall be stored in a GSA Class V or Class VI container.

### **5.6.9.3 Use of DTDs With LMP/KPs**

**Policy:** DTDs shall be operated in accordance with the LMD/KP User's Manual.

### **5.6.9.4 Audit of LMD/KP Accounts**

**Policy:** All DTDs and LMP/KPs shall be audited annually by the Treasury COR. COMSEC Custodians shall perform audits and maintain audit results for all DTDs on a monthly basis unless frequency of use requires that it be audited more frequently.

### **5.6.9.5 Training of LMD/KP Operators**

**Policy:** All operators of LMDs or LMD/KPs shall be either formally trained by NSA or its contractor or attend 6 weeks of hands-on training by an operator certified by the Treasury COR to conduct LMD/KP training.

### **5.6.9.6 Training of DTD Operators**

**Policy:** DTD operators shall be trained by the servicing COMSEC Custodian using hands-on training and the computer-based training compact disk (CD) provided by NSA.

### **5.6.9.7 Issuing Key From DTDs**

**Policy:** Keys issued from DTDs shall be reconciled weekly by the bureau COMSEC Custodian. Results of the reconciliation shall be kept on file for 3 years.

### **5.6.9.8 Security of DTDs**

**Policy:** DTDs shall be secured as any other COMSEC device in a security container when the crypto-ignition key (CIK) is installed or in a locked cabinet if the CIK has been

removed. CIK shall not be stored in the same container as the DTD unless the container meets GSA standards for storing Secret material.

#### 5.6.10 Control of Top Secret Keying Material

**Policy:** Bureaus shall safeguard Top Secret keying material using two-person integrity and no-lone zone control.

### 5.7 TEMPEST REQUIREMENTS

**Policy:** CNSS 7000, *TEMPEST Countermeasures for Facilities(s)*, shall be used to evaluate any system processing Top Secret data. A TEMPEST evaluation shall be conducted before installation and use of any system processing Top Secret information. No TEMPEST requirement exists for data classified Secret and below. Bureaus requiring a TEMPEST evaluation shall contact E-ITSPA.

### 5.8 VIRUS PROTECTION

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

- a. Installing antivirus software at the desktop that is properly configured to check all files, Internet downloads, and e-mail
- b. Installing updates to antivirus software and signature files at the desktop expeditiously and in a timely manner without requiring the end user to specifically request the update
- c. Installing security patches to servers and desktops expeditiously and in a timely manner.

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

### 5.9 PRODUCT ASSURANCE

**Policy:** In accordance with National Security Telecommunications and Information Systems Security Committee (NSTISSC) policy NSTISSP No. 11, *National Information Assurance Acquisition Policy*, January 2000:

- a. Information Assurance (IA) shall be considered as a requirement for all systems used to enter, process, store, display, or transmit classified or national security 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 also shall ensure the integrity and confidentiality of information and the authentication and nonrepudiation of parties in electronic transactions.
- b. The acquisition of all COTS IA and IA-enabled IT products to be used on systems used to enter, process, store, display, or transmit *national security information* shall be limited to only those that have been evaluated and validated in accordance with the criteria, schemes, or programs, in accordance with the following:

- 1) International Common Criteria for Information Security Technology Evaluation Mutual Recognition Agreement
  - 2) NSA/NIST National Information Assurance Partnership (NIAP) Evaluation and Validation Program
  - 3) NIST Federal Information Processing Standards (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 NSA-approved Type I cryptography products.

## 6. ACRONYMS

AES	Advanced Encryption Standard
ALC	Accounting Legend Code
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
CCI	Controlled Cryptographic Item
CD	Compact Disk
CERT	Computer Emergency Response Team
CFO	Chief Financial Officer
CFR	Code of Federal Regulations
CGI	Common Gateway Interface
CIK	Crypto-Ignition Key
CIP	Critical Infrastructure Protection
CIAO	Critical Infrastructure Assurance Officer
CIPO	Critical Infrastructure Protection Officer
CIO	Chief Information Officer
CIRB	Capital Investment Review Board
CNSS	Committee for National Security Systems
COMSEC	Communications Security
COR	Central Office of Record
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
CTS	Computerized Telephone Systems
DAA	Designated Accrediting Authority
DAIS	Defense Automatic Integrated System
DASIS	Deputy Assistant Secretary for Information Systems
DCID	Director of Central Intelligence Directive
DCS	Defense Courier Service
DES	Data Encryption Standard
DMZ	Demilitarized Zone
DO	Departmental Office
DoD	Department of Defense

DOS	Denial of Service
DRAM	Dynamic Random Access Memory
DSL	Digital Subscriber Line
DTD	Data Transfer Device
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
EKMS	Electronic Key Management System
E.O.	Executive Order
EPF	Employee Personnel File
FAM	Foreign Affairs Manual
Fax	Facsimile
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
FNBDT	Future Narrowband Digital Telephone
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
IG	Inspector General
IP	Internet Protocol
IR	Infrared

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
KP	Key Processor
LAN	Local Area Network
LMD	Local Management Device
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
NSD	National Security Directive
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
NTSWG	National Telecommunications Security Working Group
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
PIN	Personal Identification Number
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
RPC	Remote Procedure Call
RF	Radio Frequency
ROM	Read Only Memory
SA	System Administrator
SCI	Special Compartmented Information
SDLC	Software 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
STC	Sound Transmission Class
STE	Secure Telephone Equipment
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
USPS	United States Postal Service
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