UNITED STATES
DEPARTMENT OF THE TREASURY

TREASURY INFORMATION TECHNOLOGY SECURITY PROGRAM

TD P 85-01

VOLUME II
HANDBOOK

Part 1
Sensitive Systems

DOCUMENT CHANGE HISTORY

Version Number	Date	Description
1.0	June 12, 2003	Initial Release

TABLE OF CONTENTS

1. INTRODUCTION 1-1

1.1 SCOPE 1-1
1.2 AUTHORITIES 1-1
1.3 REFERENCES 1-2
1.4 POLICY OVERVIEW 1-4
1.5 DOCUMENT ORGANIZATION 1-4

2. OVERVIEW 2-1

2.1 DEFINITIONS 2-1
2.1.1 Treasury System 2-1
2.1.2 General Support System 2-1
2.1.3 Major Application 2-1
2.1.4 Mission-Critical Systems 2-1
2.1.5 National Critical Assets 2-1
2.1.6 Relationships 2-1
2.2 THREAT 2-2
2.3 DEFENSE IN DEPTH 2-3
2.4 ROLES AND RESPONSIBILITIES 2-6

3. MANAGEMENT CONTROLS 3-1

3.1 CAPITAL PLANNING AND INVESTMENT CONTROL 3-1
3.2 CONTRACTORS AND OUTSOURCED OPERATIONS 3-2
3.3 PERFORMANCE MEASURES AND METRICS 3-4
3.3.1 Performance Measures 3-4
3.3.2 Metrics 3-10
3.4 CRITICAL INFRASTRUCTURE PROTECTION 3-11
3.5 SYSTEM DEVELOPMENT LIFE CYCLE 3-12
3.6 SECURITY CHANGE MANAGEMENT 3-13
3.7 RISK MANAGEMENT 3-14
3.8 CERTIFICATION AND ACCREDITATION 3-15
3.8.1 Certification and Accreditation and Life-Cycle Management 3-15
3.8.2 Certification and Accreditation Management Issues 3-16
3.8.3 Certification 3-17
3.8.4 Accreditation 3-18
3.9 IT SECURITY REVIEW AND ASSISTANCE PROGRAM 3-20
3.10 SECURITY WORKING GROUPS AND FORUMS 3-21
3.10.1 Information Technology Security Policy Forum 3-21
3.10.2 Treasury Infrastructure Protection Panel 3-22
3.10.3 Information Technology Security Training Forum 3-22
3.10.4 CIP Working Group 3-23
3.10.5 Compliance Working Group 3-23
3.11 DISCIPLINARY ACTION 3-24

4. OPERATIONAL CONTROLS 4-1
4.1 PERSONNEL 4-1
4.1.1 Background Investigations 4-1
4.1.2 Rules of Behavior 4-2
4.1.3 Access to Sensitive Information 4-3
4.1.4 Separation of Duties 4-3
4.1.5 Training and Awareness 4-4
4.1.6 Separation From Duty 4-5
4.2 PHYSICAL SECURITY POLICIES 4-6
4.2.1 General Physical Access 4-6
4.2.2 Sensitive Facility Access 4-7
4.3 MEDIA CONTROLS 4-7
4.3.1 Media Protection 4-7
4.3.2 Media Marking 4-8
4.3.3 Sanitization 4-8
4.3.4 Production and Input/Output Controls 4-10
4.3.5 Disposal 4-10
4.4 VOICE COMMUNICATIONS 4-11
4.4.1 Private Branch Exchange 4-11
4.4.2 Telephone Communications 4-11
4.4.3 Voice Mail 4-11
4.5 DATA COMMUNICATIONS 4-12
4.5.1 Telecommunications Protection Techniques 4-12
4.5.2 Facsimile 4-12
4.5.3 Video Teleconferencing 4-13
4.5.4 Voice over IP 4-14
4.5.5 Communications Circuits 4-15
4.6 WIRELESS COMMUNICATIONS 4-15
4.6.1 Cellular Phones 4-15
4.6.2 Wireless Local Area Network 4-15
4.6.3 Pagers 4-16
4.6.4 Multifunctional Wireless Devices 4-16
4.7 OVERSEAS COMMUNICATIONS 4-17
4.8 EQUIPMENT 4-17
4.8.1 Workstation 4-17
4.8.2 Laptop Computer 4-18
4.8.3 Portable Electronic Device 4-19
4.8.4 Privately Owned Equipment and Software 4-20
4.8.5 Hardware and Software Maintenance 4-20
4.9 CONVERGING TECHNOLOGIES 4-20
4.10 GENERAL IT SECURITY 4-21
4.10.1 Security Incident and Violation Handling 4-21
4.10.2 Contingency Planning 4-23
4.10.3 Documentation (Manuals, Network Diagrams) 4-25
4.10.4 Information Backup 4-25

5. TECHNICAL CONTROLS 5-1
5.1 IDENTIFICATION AND AUTHENTICATION 5-1
5.1.1 Passwords 5-1
5.2 ACCESS CONTROL 5-2
5.2.1 Automatic Account Lockout 5-2
5.2.2 Automatic Session Lockout 5-2
5.2.3 Warning Banner 5-2
5.3 AUDIT TRAIL 5-7
5.4 NETWORK SECURITY 5-7
5.4.1 Remote Access 5-7
5.4.2 Network Security Monitoring 5-8
5.4.3 Network Connectivity 5-9
5.4.4 Firewalls 5-9
5.4.5 Internet Security 5-11
5.4.6 Electronic Mail Security 5-14
5.4.7 Privately Owned E-Mail Accounts 5-15
5.4.8 Penetration Testing and Vulnerability Assessment 5-15
5.5 CRYPTOGRAPHY 5-16
5.5.1 Encryption 5-16
5.5.2 Public Key Infrastructure 5-16
5.5.3 Public Key/Private Key 5-21
5.6 VIRUS PROTECTION 5-21
5.7 PRODUCT ASSURANCE 5-22

6. INCIDENT RESPONSE PROCEDURES 6-1
6.1 INCIDENT RESPONSE CAPABILITY OVERVIEW 6-1
6.1.1 Treasury Incident Response Capability Structure 6-1
6.1.2 TCSIRC Functions 6-2
6.1.3 Incident Reporting Process Flow 6-3
6.1.4 Incident Priority Levels 6-3
6.1.5 Incident Response Definitions 6-4
6.1.6 Roles and Responsibilities 6-5
6.2 INCIDENT REPORTING REQUIREMENTS 6-7
6.2.1 TCSIRC Reporting Requirements 6-7
6.2.2 Bureau CSIRC Reporting Requirements 6-9
6.3 INCIDENT HANDLING 6-12
6.3.1 Bureau CSIRC Support 6-12
6.3.2 TCSIRC Support 6-14
6.3.3 Onsite Incident Handling 6-15
6.4 INCIDENT PREVENTION REQUIREMENTS 6-16
6.4.1 Bureau CSIRC Responsibilities 6-16
6.4.2 TCSIRC Responsibilities 6-16

7. ACRONYMS 7-1

8. DEFINITIONS 8-1

APPENDIX A—TCSIRC CONTACT INFORMATION A-1
APPENDIX B—RESPONSE GUIDELINES B-1
APPENDIX C—TREASURY SECURITY INCIDENT REPORT FORM C-1
APPENDIX D—SAMPLE BUREAU MONTHLY SUMMARY REPORT D-1
APPENDIX E—DEFINITIONS OF TREASURY SECURITY INCIDENTS E-1
APPENDIX F—GLOSSARY F-1

TABLE OF FIGURES

Figure 2-1. Relationships Among System Types 2-2
Figure 2-2. Defense-in-Depth Strategy 2-3
Figure 6-1. TCSIRC Structure 6-2
Figure 6-2. Incident Reporting Process Flow 6-3

TABLE OF TABLES

Table 2-1. Threat Summary 2-2
Table 2-2. Examples of Layered Defenses 2-6
Table 3-1. Examples of IT Security Costs 3-1
Table 3-2. Example of Proposal to Determine Risk Levels 3-15
Table 4-1. Examples of Minimum Background Investigations 4-1
Table 4-2. Clearing and Sanitization Matrix 4-9
Table 6-1. Incident Priority Levels 6-3

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' IT security programs. The standards in this volume are binding on all Treasury bureaus and offices; the procedures are intended as guidance.

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.

Treasury Directive (TD) P 85-01 is issued under the authority of TD 85-01, *Department of the Treasury Information Technology 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 through 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 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 Treasury Inspector General for Tax Administration (TIGTA), hereafter referred to collectively as "bureaus." This document provides standards and procedures that relate to management, operational, and technical controls. These controls provide the foundation for ensuring confidentiality, integrity, availability, reliability, and nonrepudiation within the Department of the Treasury's IT infrastructure and operations.

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

1.2 AUTHORITIES

The Department of the Treasury has established a departmentwide IT security program and organization based on the following Executive orders, public laws, national policy, and Department of the Treasury orders.

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*, November 28, 2000.

c. OMB Circular A-11, *Preparing, Submitting, and Executing the Budget*, updated annually.

d. OMB Circular A-123, *Management Accountability and Control*, June 21, 1995.

e. OMB Circular A-127, *Financial Management Systems*, July 23, 1993.

f. Public Law 104-106, Clinger-Cohen Act of 1996 [formally, Information Technology Management Reform Act (ITMRA)], February 10, 1996.

g. E.O. 13231, *Critical Infrastructure Protection in the Information Age*, October 16, 2001, as amended February 28, 2003, Executive Orders, Amendments of Executive Orders, and other Laws in connection with the establishment of the Department of Homeland Security.

h. Presidential Decision Directive (PDD) 63, *Critical Infrastructure Protection*, May 1998.

i. 5 Code of Federal Regulations (CFR) §2635, Office of Government Ethics, *Standards of Ethical Conduct for Employees of the Executive Branch*.

j. Public Law 93-502, Freedom of Information Act (FOIA) of 1980.

k. Public Law 99-474, Computer Fraud and Abuse Act.

l. Department of State 12 Foreign Affairs Manual (FAM) 600, *Information Security Technology*, June 22, 2000.

m. Treasury Order (TO) 106-09, *Electronic Funds and Securities Transfer Policy—Message Authentication and Enhanced Security*, October 2, 1986.

n. 41 United States Code (U.S.C.) §423, Procurement Integrity Act.

o. 26 U.S.C. §6103, Internal Revenue Code.

1.3 REFERENCES

a. International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 15408, *Common Criteria for Information Technology Security Evaluation.*

b. American National Standards Institute (ANSI) X9.9, *Financial Institution Message Authentication*, April 13, 1982.

c. National Institute of Standards and Technology (NIST) Computer Security Resource Center (CSRC) Federal Information Processing Standards (FIPS), http://csrc.nist.gov, publications, Federal Information Processing Standards link.

d. NIST CSRC Special Publications (SP), http://csrc.nist.gov, publications, Special Publications link.

e. NIST CSRC Information Technology Laboratory (ITL) Computer Security Bulletins, http://csrc.nist.gov, publications, ITL bulletins link.

f. General Accounting Office (GAO), Federal Information System Controls Audit Manual (FISCAM).

g. National Computer Security Center (NCSC), NCSC-TG-025, *A Guide to Understanding Data Remanence in Automated Information Systems*, Version 2, September 1991.

h. National Security Telecommunications and Information Systems Security (NSTISS) Directive (NSTISSD) 500, *Information Systems Security (INFOSEC) Education, Training, and Awareness*, February 25, 1993.

i. NSTISSD 501, National Training Program for Information Systems Security (INFOSEC) Professionals, November 16, 1992.

j. NSTISS Instruction (NSTISSI) No. 1000, National Information Assurance Certification and Accreditation Process (NIACAP), April 2000.

k. NSTISSI, National Training Standards, http://www.nstissc.gov, library.

l. OMB Memorandum M-99-18, *Privacy Policies for Federal Web Sites*, June 2, 1999.

m. OMB Memorandum M-99-20, Security of Federal Automated Information Resources, June 23, 1999.

n. OMB Memorandum M-00-07, Incorporating and Funding Security in Information Systems Investments, February 28, 2000.

o. OMB Memorandum M-01-08, Guidance on Implementing the Government Information Security Reform Act, January 16, 2001.

p. OMB Memorandum M-02-09, Reporting Instructions for the Government Information Security Reform Act and Updated Guidance on Security Plans of Action and Milestones, July 2, 2002.

q. TD 71-10, *Department of the Treasury Security Manual*, and associated manual TD P 71-10, April 9, 2001.

r. TD 74-14, Treasury Telework and Flexiplace Program, October 18, 2000.

s. TD 80-05, *Records and Information Management Manual*, and associated manual TD P 80-05, February 23, 2000.

t. TD 81-01, *Treasury Information Technology Programs*, and associated manual TD P 81-01, April 13, 2000.

u. TD 81-08, Certification Process for the Use of Persistent Cookies on Treasury Web Sites, January 10, 2002.

v. TD 84-01, *Information System Life Cycle*, and associated manual TD P 84-01, March 7, 2002.

w. TD 86-04, Authorized Use of Government Telephone Services.

x. TD 87-05, Electronic Commerce Initiatives, April 21, 2001.

y. Department of the Treasury, Treasury Critical Infrastructure Protection: Interdependency Analysis Methodology, Version 1.1, September 24, 2002.

z. Department of the Treasury, *Treasury Critical Infrastructure Protection Plan* (TCIPP), Version 2.

aa. Department of the Treasury, Security Classification Guide for the Department of the Treasury's Critical Information Assets Associated with Project Matrix, February 20, 2002.

bb. Department of the Treasury, Security Control Guide for the Department of the Treasury's Sensitive Critical Information Assets Associated with Project Matrix, February 1, 2002.

1.4 POLICY OVERVIEW

A policy delineates the security management structure, assigns responsibilities, and lays the foundation necessary to measure progress and compliance. The standards and procedures in Treasury IT Security Program, Volume II, correspond to the policies in Volume I. The standards and procedures are subdivided into 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 are normally addressed by management.

b. **Operational Controls.** Address security methods focusing on the mechanisms primarily implemented and executed by people. These controls are established to improve the security of a group, a particular system, or a group of systems. These controls require technical or specialized expertise and rely on management and technical controls.

c. **Technical Controls**. Focus on security controls that a computer system executes. These controls can provide automated protection for unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data.

1.5 DOCUMENT ORGANIZATION

TD P 85-01, Treasury IT Security Program, is subdivided 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 the 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 II, Treasury IT Security Program Handbook, Part 1, Sensitive Systems, is described below. In Sections 3 through 5, standards are mandatory, procedures are guidelines.

- Section 1 provides the scope, the authorities, an overview, and the structure of the document.
- Section 2 presents descriptions of roles, responsibilities, and threats.
- Section 3 presents the standards and procedures relating to management controls, such as risk management and capital investment planning.
- Section 4 presents the standards and procedures relating to operational controls, such as personnel and disaster recovery.
- Section 5 presents the standards and procedures relating to technical controls, such as identification and authentication (I&A) and network security.
- Section 6 provides the Incident Response Procedures Guide.
- Section 7 provides a list of the acronyms used within this manual
- Section 8 provides a glossary of the terms used within this manual.

2. OVERVIEW

This section defines the types of systems, discusses the threat, and lists detailed responsibilities for each role.

2.1 DEFINITIONS

2.1.1 Treasury System

A Treasury system is IT that is a) owned, leased, or operated by a bureau, DO, OIG, TIGTA, or a component thereof or b) operated by a contractor on behalf of a bureau, DO, OIG, TIGTA, or a component thereof.

2.1.2 General Support System

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

2.1.3 Major Application

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

2.1.4 Mission-Critical Systems

A mission-critical system is a system that is essential for the performance of the organization's mission.

2.1.5 National Critical Assets

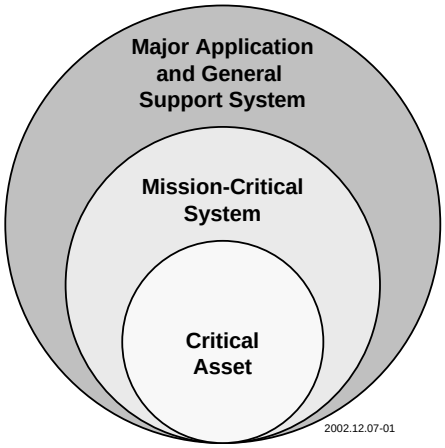
A national critical asset is a system that is essential to the minimum operations of the economy and the Government.

2.1.6 Relationships

Figure 2-1 illustrates the relationships among major applications/general support systems, mission-critical systems, and critical assets. A critical asset is essential to the minimum

operations of the national infrastructure. It will also be a mission-critical system and a major application or general support system. A mission-critical system will be a major application or a general support system.

Figure 2-1. Relationships Among System Types



2.2 THREAT

Volume I provides information on threats. The discussion below will assist in determining the level of risk from these specific threats.

To effectively resist attacks on its information and information systems, an organization must characterize its adversaries, their potential motivations, and their attack capabilities. Potential adversaries might include nation states, terrorists, criminal elements, hackers, or corporate competitors. Their motivations might include intelligence gathering, theft of intellectual property, causing embarrassment, or just anticipated pride in having exploited a notable target. The methods of attack might include passive monitoring of communications, active network attacks, close-in attacks, exploitation of insiders, and attacks through the industry providers of the organization's IT system resources.

Table 2-1 summarizes the threat. Adversaries with low or no fear of detection are most likely to attack.

Table 2-1. Threat Summary

Adversary	Technical Capability	Monetary Resources	Fear of Detection
Hacker	Low	Low	Low
Experienced Hacker	Medium	Low	Medium
Terrorist	Medium	Medium	Very Low
Criminal	Medium	High	Medium
Rogue Nation State	Medium	High	Peace: Low War: None
Nation State	High	High	Peace: High War: None

Malicious insiders may be agents of some adversaries.

In addition to guarding against intentional attack, the organization must protect against the detrimental effects of nonmalicious events such as fire, flood, power outages, and user error.

When determining risks from these threats, it is important to focus on actual threat versus perceived threat.

2.3 DEFENSE IN DEPTH

The Department of the Treasury endorses a defense-in-depth concept. The following paragraphs describe this concept.

Information assurance (IA) is achieved when there is confidence that information and information technology are protected against attacks through the application of security services in such areas as availability, integrity, authentication, confidentiality, and nonrepudiation. The application of these services should be based on the protect, detect, and react paradigm. This means that in addition to incorporating protection mechanisms, organizations must expect attacks and must also incorporate attack-detection tools and procedures that allow them to react to and recover from these attacks.

Figure 2-2 illustrates an important principle of the defense-in-depth strategy: the achievement of IA requires a balanced focus on three primary elements: people, technology, and operations.

Figure 2-2. Defense-in-Depth Strategy

The achievement of IA begins with a senior-level management commitment (typically at the Chief Information Officer [CIO] level) based on a clear understanding of the perceived threat. This commitment must be followed by establishment of effective IA policies and procedures, assignment of roles and responsibilities, commitment of resources, training of critical personnel (e.g., users and system administrators), and enforcement of personal accountability. These elements include the establishment of physical security and personnel security measures to control and monitor access to facilities and critical elements of the IT system environment.

A wide range of technologies are available for providing IA services and for detecting intrusions. To ensure that the right technologies are procured and deployed, an organization should establish effective policies and processes for technology acquisition. These policies and processes should include security policy, IA principles, system-level IA architectures and standards, criteria for needed IA products, acquisition of products that have been validated by a reputable third party, configuration guidance, and processes for assessing the risk of the integrated systems.

The operations element of the strategy focuses on all activities required to sustain an organization's security posture on a day-to-day basis.

There are four defense-in-depth technology focus areas: defend the computing environment, defend the enclave boundaries, defend the networks and infrastructure, and defend supporting infrastructures.

The defense-in-depth strategy recommends adherence to several IA principles:

a. **Defense in Multiple Places.** Given that adversaries can attack a target from multiple points using insiders or outsiders, an organization must deploy protection mechanisms at multiple locations to resist all methods of attack.

   At a minimum, these defense-in-depth locations should include—

   1) Defend the networks and infrastructure.

      a) Protect LANs and wide area networks (WAN) (e.g., from denial-of-service [DoS] attacks).

      b) Provide confidentiality and integrity protection for data transmitted over these networks (e.g., use encryption and traffic flow security measures to resist passive monitoring).

      c) Ensure that all data exchanged over WAN is protected from disclosure to anyone not authorized to access the network.

      d) Ensure that WANs supporting mission-critical and mission-support data provide appropriate protection against DoS attacks.

      e) Protect against the delay, misdelivery, or nondelivery of otherwise adequately protected information.

      f) Protect against traffic flow analysis—
         - User traffic.
         - Network infrastructure control information.

      g) Ensure that protection mechanisms do not interfere with otherwise seamless operation with other authorized backbone and enclave networks.

   2) Defend the enclave boundaries (e.g., deploy firewalls and intrusion detection to resist active network attacks).

      a) Ensure that physical and logical enclaves are adequately protected.

b) Enable dynamic throttling of services in response to changing threats.

c) Ensure that systems and networks within protected enclaves maintain acceptable availability and are adequately defended against DoS intrusions.

d) Ensure that data exchanged between enclaves or via remote access is protected from improper disclosure.

e) Provide boundary defenses for those systems within the enclave that cannot defend themselves as a result of technical or configuration problems.

f) Provide a risk-managed means of selectively allowing essential information to flow across the enclave boundary.

g) Provide protection against the undermining of systems and data within the protected enclave by external systems or forces.

h) Provide strong authentication, and thereby authenticated access control, of users sending or receiving information from outside their enclave.

3) Defend the computing environment (e.g., provide access controls on hosts and servers to resist insider, close-in, and distribution attacks).

a) Ensure that clients, servers, and applications are adequately defended against DoS, unauthorized disclosure, and modification of data.

b) Ensure the confidentiality and integrity of data processed by the client, server, or application inside and outside the enclave.

c) Defend against the unauthorized use of a client, server, or application.

d) Ensure that clients and servers follow secure configuration guidelines and have all appropriate patches applied.

e) Maintain configuration management of all clients and servers to track patches and system configuration changes.

f) Ensure that a variety of applications can be readily integrated with no reduction in security.

g) Ensure adequate defenses against subversive acts by trusted persons and systems, both internal and external.

b. **Layered Defenses.** Even the best available IA products have inherent weaknesses. Consequently, an adversary will eventually find an exploitable vulnerability in almost any system. An effective countermeasure is to deploy multiple defense mechanisms between adversaries and their target. Each mechanism must present unique obstacles to the adversary. Further, each should include protection and detection measures. These measures help to increase risk (of detection) for the adversary while reducing his or her chances of success or making successful penetrations unaffordable. Deploying nested firewalls (each coupled with intrusion detection) at outer and inner network boundaries is an example of a layered defense. The inner firewalls may support more granular access control and data filtering. Table 2-2 provides other examples of layered defenses.

Table 2-2. Examples of Layered Defenses

Class of Attack	First Line of Defense	Second Line of Defense
Passive	Link and network layer and encryption and traffic flow security	Security-enabled applications
Active	Defense of the enclave boundaries	Defense of the computing environment
Insider	Physical and personnel security	Authenticated access controls, audit
Close-in	Physical and personnel security	Technical surveillance countermeasures
Distribution	Trusted software development and distribution	Run-time integrity controls

c. **Security Robustness.** Specify the security robustness (strength and assurance) of each IA component as a function of the value of what it protects and the threat at the point of application.

d. **Deploy Key Management Infrastructure/Public Key Infrastructure (KMI/PKI).** Deploy robust KMI and PKI that support all of the incorporated IA technologies and that are highly resistant to attack. Provide a cryptographic infrastructure that supports key, privilege, and certificate management and that enables positive identification of individuals using network services.

e. **Deploy Intrusion Detection Systems (IDS).** Deploy infrastructures to detect intrusions, to analyze and correlate the results, and to react as needed. These infrastructures should help the operations staff answer questions such as, Am I under attack? Who is the source? What is the target? Who else is under attack? What are my options?

   1) Provide an intrusion detection, reporting, analysis, assessment, and response infrastructure that not only enables rapid detection and response to intrusions and other anomalous events but also provides operational situation awareness.

   2) Plan execution and reporting requirements for contingencies and reconstitution.

2.4 ROLES AND RESPONSIBILITIES

Refer to Volume I, Part 1, for the basic high-level responsibilities. This section provides additional details.

a. The Assistant Secretary for Management and Chief Financial Officer (ASM/CFO) shall—

   1) Ensure that adequate resources are provided for the IT security program departmentwide and at the bureau level.

   2) Serve as IT security champion within the Department of the Treasury.

   3) Ensure that a Designated Accrediting Authority (DAA) is appointed for each enterprisewide application. Designate the DAA for enterprisewide applications supporting ASM/CFO programs.

4) Ensure the appointment of a Treasury Critical Infrastructure Assurance Officer (CIAO) who shall oversee the planning, development, and implementation of critical infrastructure protection (CIP) and assurance requirements departmentwide.

5) Oversee the activities of the Treasury CIAO to ensure the effectiveness of planning and implementation activities for protecting and assuring Treasury Critical Infrastructure (TCI).

6) Ensure that mission areas identify and prioritize critical assets for protection and assurance, including recovery and reconstitution.

b. The Deputy Assistant Secretary for Information Systems (DASIS)/CIO shall—

1) Ensure that the departmentwide IT security program is adequately resourced.

2) Delegate to the Director, Enterprise IT Security Planning and Assurance (E-ITSPA), the responsibility for the implementation and maintenance of the departmentwide IT security program.

3) Approve the yearly IT security program report for OMB.

4) Coordinate with the departmental offices, bureaus, and the National Communications System the identification of National Information Infrastructure assets critical to Treasury operations, and national security and emergency preparedness communications.

5) Ensure the implementation and maintenance of a response and recovery capability within the Department for Treasury-critical national functions and their infrastructures, and ensure an interface with related activities of federal, state, and local governments and private industry.

c. The Treasury CIAO shall—

1) Serve as the Treasury CIAO. The CIAO is responsible for departmental policy regarding the protection of Treasury's critical infrastructures.

2) Chair the Treasury Infrastructure Protection Panel (TIPP), a senior Treasury steering committee.

3) Ensure the appointment of a Treasury Critical Infrastructure Protection Officer (CIPO) who shall coordinate the planning, development, and implementation of CIP requirements departmentwide.

d. The Director, E-ITSPA, shall—

1) Develop and prescribe policy, standards, techniques, and guidelines for the security, protection, accountability, and integrity of the Department's sensitive IT system.

2) Establish and maintain a departmental IT threat database and provide threat briefings and threat assessments to bureaus.

3) Facilitate IT security awareness and training programs throughout the Department of the Treasury.

4) Establish and conduct an IT security oversight program that includes a review of bureau policies, plans, and budgets to ensure that bureau IT security programs are in compliance with national and Treasury policies.

5) Resolve any conflicting security issues that occur where an IT system substantially involves more than one DAA.

6) Be responsible for certain reserved functions, including those required by FISMA and those falling under the DASIS/CIO.

7) Review for consideration requests for exceptions to policies and standards in the Treasury IT Security Program.

8) Represent Treasury in external policy and standards setting forums, professional organizations, and private enterprise to influence IT security policy developments that will affect Treasury.

9) Prepare the Department of the Treasury annual report in accordance with FISMA and OMB instructions.

10) Collect and track all IT security weaknesses in a Plan of Action and Milestones (POA&M). Validate the completion of all milestones. Provide updates on the POA&M to OMB quarterly through the Treasury CIO.

11) Establish performance metrics to track the implementation of the departmentwide IT security program.

e. The ASM/CFO, heads of bureaus, OIG, and TIGTA shall—

1) Issue bureau policies as needed to implement the Department of the Treasury IT Security Program.

2) Establish bureau security programs.

3) Certify that adequate security exists for bureau IT systems and describe security and other material weaknesses in these systems in the bureau head's annual report to the Secretary under TD 40-04.

4) Ensure that adequate controls are in place, as required by OMB Circulars A-130, A-123, and A-127.

5) Designate or ensure designation of DAAs for their respective offices. Where an IT system substantially involves more than one bureau, a single DAA should be designated the accrediting authority by mutual agreement with the approval of the Director, E-ITSPA.

6) Designate a CIO with appropriate authority and responsibility to manage the sensitive IT security program for the bureau.

7) Establish formal memorandums of understanding (MOU) among external agencies' accrediting authorities before allowing telecommunications interconnections of accredited IT systems. The MOU shall stipulate all the terms and conditions of the security arrangements that will govern the operation of the interconnected network of IT systems.

8) Establish, when appropriate, their own security organizations and position designations, provided that the responsibilities and functions outlined herein are officially assigned and performed.

9) Ensure the appointment of a bureau CIAO, who shall coordinate the planning, development, and implementation of CIP/assurance requirements bureauwide.

10) Oversee the activities of the bureau CIAO to ensure the effectiveness of planning and implementation activities for protecting and assuring TCI.

11) Report the status of the Treasury CIP capability to the Treasury CIAO and the Treasury CIPO.

f. The DAA shall be a senior management official who manages a Treasury mission or function supported by IT systems or who has authority to evaluate the overall mission requirements of IT systems. The DAA shall—

1) Manage a U.S. Treasury or bureau mission or function supported by an IT system or have authority to evaluate the overall mission requirements of the IT system.

2) Determine information sensitivity.

3) Coordinate with the CIO regarding the security requirements of the sensitive information and provide definitive directions to IT developers or owners relative to the risk in the security posture of the IT system.

4) Decide on accepting the minimum security safeguards prescribed for an IT system.

5) Implement all applicable protection policies prescribed by the Treasury and bureau CIO.

6) Execute a statement that an IT system is accredited and accept accountability for the residual risks assumed.

7) Ensure that risk analysis responsibilities are accomplished in accordance with this policy.

g. The Program Officials shall—

1) Ensure that the budget and business cases for the IT supporting their program provide adequate funding for IT security.

2) Appoint an Information Systems Security Officer (ISSO) for the IT systems supporting their program.

3) Ensure that performance measures and metrics are established for their IT security program.

4) Ensure that the IT security program is reviewed annually.

5) Report the results of the IT security program review, including any weaknesses, to their bureau CIO for inclusion in the bureau's POA&M.

h. The bureau CIO shall—

1) Manage the sensitive IT security program for the bureau.

2) Ensure certification of the implementation of technical and nontechnical security safeguards for a sensitive IT system and facility to the appropriate DAA with a statement of the level of risk.

3) Ensure that the responsibilities for carrying out the Treasury IT Security Program are appropriately assigned within the bureau or office.

4) Designate a bureau employee as an Information Systems Security Manager (ISSM) who is responsible for managing and overseeing the bureau IT security program.

5) Designate representatives and their backups for participation in forums and working groups, in accordance with the policy defined in TD P 85-01, Volume I, Part 1, Section 3.10, and the standards defined in this document.

6) Prescribe and advise the DAA on the appropriate Department of the Treasury and bureau protection policies.

7) Ensure that all protection techniques are cost effective and consistent with the policies in this Treasury IT Security Program Handbook.

8) Manage a security awareness and training program for bureau and contractor personnel working with bureau or office IT.

9) Coordinate the IT security program with the internal control and accounting system evaluation programs under the Federal Managers' Financial Integrity Act to avoid duplication and to ensure that the objectives of each program are met.

10) Establish performance measures and metrics for the bureau IT security program.

11) Ensure that bureau programs are reviewed annually.

12) Provide an annual report, in accordance with FISMA, to the Treasury CIO.

13) Provide quarterly updates of the bureau POA&M to E-ITSPA.

i. The bureau CIAO shall—

1) Ensure the appointment of a bureau CIPO, who will be responsible for addressing bureau programmatic requirements and issues.

2) Prepare and submit budget requests to establish and maintain CIP within the bureau.

3) Identify the critical national and sector-related banking and financial functions performed by the bureau, and the IT systems, emergency preparedness communications, and physical assets and facilities used in supporting national security and national economic security missions.

4) Work with the Treasury CIAO/CIPO in using Project Matrix to establish and maintain a prioritized inventory of the Treasury bureau's TCI; to identify bureaus' interdependencies with other federal, state, and local agencies; and to identify dependencies on the private sector.

j) The ISSM shall—

1) Prepare and distribute bureau policies, standards, and guidelines as necessary to implement the Treasury IT Security Program, and monitor their implementation.

2) Establish a security awareness and training program, including tracking the funds expended, the courses taken, and the personnel who received the training and their positions.

3) Ensure that IT system certification and accreditation (C&A) reports and risk analyses are conducted as required.

4) Review bureau business cases and budget submissions to ensure that IT security requirements are addressed and adequately resourced.

5) Establish a bureau IT security oversight program to ensure that the security procedures and requirements are in compliance with Treasury and bureau policies and standards. Conduct security audits, verifications, and acceptance checks and maintain documentation on the results.

6) Maintain bureau POA&M on all IT security weaknesses. Provide the quarterly status to E-ITSPA through the bureau CIO.

7) Evaluate the security impact of any facility-unique patches or system modification and approve those that do not adversely affect system security.

8) Monitor system use periodically; inspect and monitor user files only with appropriate approval.

9) Coordinate the implementation of logical access controls into operating systems, database management systems, remote terminals, and IT applications.

10) Provide IT and facility technical and nontechnical certification support.

11) Prepare and submit a written report to the CIO for all technical security exceptions. The report shall outline the risks and vulnerabilities and/or advantages that could result from granting the exception or from implementing any alternative. Maintain a file of all approved IT facility security-related exceptions.

12) Ensure that security plans are reviewed annually to ensure that they are complete and up to date and that updated plans are submitted to the DAA for approval.

13) Ensure that a risk analysis is conducted at least every 3 years or when a major change occurs for IT systems processing sensitive information.

14) Ensure that contingency plans for IT systems processing sensitive information are developed, maintained, and tested.

15) Ensure that a security test and evaluation (ST&E) is performed for each sensitive system being developed and reviewed, as necessary as part of the C&A process.

16) Serve on the Configuration Control Board (CCB). Evaluate the impact of changes on the security posture of the IT system and provide the report to the CCB.

k. The ISSO shall—

1) Perform evaluations of the technical and nontechnical security features of IT and other safeguards in support of the accreditation process.

2) Ensure compliance with the security requirements of the IT system.

3) Ensure that all applicable bureau information system security policies, Treasury IT Security Program directives, and other applicable directives are properly implemented for the systems and at the facilities under his or her purview.

4) Implement the security requirements defined for the sensitive information processed by the IT systems facility.

5) Coordinate IT systems facility changes with the bureau CIO and DAA.

6) Ensure that security testing is accomplished for certification purposes after installing a product. This testing shall guarantee that the product functions as intended with a particular bureau application or system.

7) Ensure that any remote facility is in compliance with all applicable security policies and procedures.

8) Implement security procedures to control access to remote devices under his or her control.

9) Ensure that all personnel who install, operate, maintain, or use the IT system have been authorized access to use the IT system, are familiar with documented security practices before they gain access to the IT system, and have acknowledged in writing applicable system security requirements and responsibilities.

10) Develop; review; and submit for approval to the CIO, DAA, or other appropriate bureau official the procedures for reporting, investigating, and resolving all IT security incidents involving the ISSO's IT system, facility, and Treasury remote locations.

11) Develop; review; submit for approval to the CIO, DAA, or other appropriate bureau official; and implement procedures for monitoring and reacting to system security alarms, warning messages, and reports.

12) Develop, review, and implement procedures for IT facility access control.

13) Monitor system procedures for hardware and software configuration control and access to system tapes, disks, and software patches.

14) Serve on Change Review Board (CRB). Evaluate the impact of changes on the security posture of the IT system and provide the report to the CRB.

15) Review system and related software security vulnerabilities.

16) Conduct system fault analyses, as required, and participate in the preparation of incident reports.

17) Initiate protective or corrective measures if a security problem develops.

18) Report security incidents, in accordance with Section 6 of this document, to the bureau incident response capability, the bureau CIO, and the DAA, and report the security status of the affected IT system.

19) Evaluate the effectiveness and impact of the security measures and features and report existing or potential problem areas to the bureau CIO and DAA.

20) Examine system audit trails regularly and report anomalies to the bureau incident response capability and the DAA.

21) Ensure that tests of the security protective features are performed after each significant system change and maintain test documentation.

22) Maintain documentation detailing the IT hardware and software configuration control and all security countermeasures that protect it.

23) Maintain a record of visitors to central IT facilities.

l. The Treasury CIPO shall—

1) Ensure the proper coordination, planning, implementation, and oversight of CIP and assurance activities within the Department.

2) Establish and maintain a collective list of Treasury banking and financial critical infrastructure.

3) Oversee and ensure CIP-related policy and legislative compliance by each bureau.

4) Report CIP Program activity and progress to the TIPP.

m. The bureau CIPO shall—

1) Ensure the proper coordination, planning, implementation, and oversight of CIP and assurance activities within the bureau. This multifaceted coordination requires interaction and consensus building with infrastructure asset owners, program managers, business managers, IT personnel, facilities management, human resources, and various security personnel.

2) Support the Treasury CIPO in reporting program activity and progress to the TIPP.

n. The Department of the Treasury employees and contractors, and any users of Treasury IT systems shall—

1) Comply with all executive, legislative, and Treasury and bureau security policies and procedures.

2) Minimize the threat of viruses by write-protecting diskettes, routinely scanning files and systems for viruses, and never circumventing antivirus safeguards.

3) Report any suspicious or unusual activity to the appropriate supervisor, ISSO, or incident response capability.

4) Attend an initial security briefing and acknowledge attendance at the security briefing in writing.

5) Attend periodic (at least annual) refresher training.

6) Thoroughly read and abide by the Rules of Behavior for the systems, as well as associated policies and procedures to which personnel are granted access.

3. MANAGEMENT CONTROLS

3.1 CAPITAL PLANNING AND INVESTMENT CONTROL

OMB requires reports on IT investments for several reasons. Ultimately, OMB must justify to Congress how money is allocated through the capital planning process. OMB ensures that the Federal Government's limited funds are applied toward the most critical and best-protected assets and programs.

Recognizing the importance of IT capital investments to the organization, and Treasury's role in supporting the success of these investments, Treasury is engaged in an effort to maintain and support a comprehensive IT capital investment analysis and decisionmaking environment. This environment consists of three key components: executive decisionmakers, supporting tools, and repeatable processes.

Members of the Treasury Capital Investment Review Board (CIRB) or the equivalent are the primary executive decisionmakers. At the bureau level, an investment review board (or an equivalent group) oversees the bureau's IT capital investments. The Department of the Treasury shall establish cross-functional team(s) to support the CIRB's decisions and oversee investments through their life cycle.

a. **Standards**

1) E-ITSPA shall establish a process to review business cases placed before the Treasury CIRB for adequate security. E-ITSPA shall participate in the Exhibit 300 review process to ensure that the IT security questions are adequately addressed for each IT capital investment.

2) Program Officials shall ensure that security requirements for the applications supporting their program are adequately resourced and that their Exhibit 300 reflects these requirements and resources.

b. **Procedures**

Table 3-1 lists items to consider, in addition to the purchase of the technology, in developing business cases and Exhibit 300 costs for IT security.

Table 3-1. Examples of IT Security Costs

Item	Requirement	Cost Estimate
ISSO and backup ISSO	Full-time equivalent (FTE) or contractor support	GS-13 or GS-14 salary and benefits
Contractor support		$250,000 per staff year + 10% fee
Background investigations	Required for FTE and contractors, updated every 5 years	Average $3,600 each
Security administrator	Manages user accounts; reviews audit logs	Contractor or GS-12 or GS-13 FTE
Database administrator	Ensures that database security is appropriately implemented	Contractor or GS-13 or GS-14 FTE

Item	Requirement	Cost Estimate
Firewall or IDS administrator	Manages configuration of firewall or IDS; reviews alarms and logs	Contractor or GS-13 or -14 FTE
C&A	Required before implementation, updated at major change or at least every 3 years	$100,000–$450,000, depending on the complexity and sensitivity of the system
Vulnerability and penetration testing	Required annually for critical assets; should be performed quarterly on networks	$50,000–$75,000
Registration Authority	If using public key certificates, need a registration authority to validate requests for these certificates	Contractor or GS-11 or GS-12
Specialized IT security training courses	Required to maintain skills of IT security personnel	For contractors, include as part of the overhead for the contract; for FTE, course costs range from $2,000 to $3,000 each

The Program Official must determine the number of persons required for each area on the basis of the size of the system and the required hours of operation. For example, the ISSO, although a single *role*, is not just one *person*, because a backup would be needed when the ISSO was on leave or at training. In addition, 24-hour-a-day operations require personnel for each shift.

The costs of security equipment and software can be obtained from vendors. Maintenance costs are typically 10 to 15 percent of the purchase price.

These costs need to be projected for the life cycle of the system (typically, 3 years for hardware and 5 years for IT applications).

3.2 CONTRACTORS AND OUTSOURCED OPERATIONS

All Treasury officials are responsible for protecting sensitive information and assets under their control. This responsibility applies not only to all phases of the contracting process, including bidding, negotiating, awarding, performance, and termination of contracts, but also to internal government operations.

IT security shares properties with systems and software engineering, including trustworthiness, system safety, and reliability. Federal information processing procurement is the process of acquiring hardware, software, firmware, computer-related services, and telecommunications. Federal information processing procurement begins with the process of determining needs and ends with contract completion.

The integration of IT security and Federal information processing procurement will result in improvements in—

- Meeting agency missions
- Protecting federal assets
- Protecting individual rights.

The integration is accomplished by incorporating IT security into all phases of the procurement cycle: planning, solicitation, source selection, and contract administration and closeout.

a. **Standards**

1) Identify security requirements that the contractor and outsourced operations shall meet in addition to those related to the specific technology.

2) The bureaus shall write the security requirements into the contract work statement. Include explicit procedures where necessary.

3) Assess the contractor's and outsourced operations' capability to meet the Department of the Treasury's security requirements. The source selection plan shall assess the contractor's ability to meet the security requirements stated.

4) The bureaus shall identify and provide the information and resources that are specifically required for an outside contractor to perform contracted services and shall prohibit access to all other information.

5) Identify and document in the statement of work (SOW) how the Department of the Treasury's information is to be handled and protected at the contractor's facility or site. Contractor operations shall adhere to the Department of the Treasury and bureau security policy.

6) The bureaus shall ensure that, at the expiration of contract, contractors certify that they sanitize Treasury information from any contractor-owned system used to process Treasury information and shall ensure the return of any Treasury IT resources provided to the contractor.

7) When work is performed at the contractor's facility, the bureau shall annually conduct a review of its facility and IT security procedures.

8) The ISSM shall review all contracts before award to ensure that IT security requirements have been incorporated.

b. **Procedures**

The following issues at a minimum should be addressed in the SOW:

1) What level of background investigation is required, and what actions are required of the contractor to obtain the background investigation?

2) Do the contract employees need to be U.S. citizens?

3) Will the work be performed at your facility or at the contractor's facility?

4) What equipment and software will you provide the contractor?

5) If the contractor uses its own equipment, what procedures must it follow to safeguard your information? Be sure to consider maintenance and disposal of the equipment in these requirements. Will you permit the contractor to connect to your network? What procedures should the contractor follow to protect any sensitive information transmitted by electronic mail (e-mail)?

6) Ensure that the contractor provides any specialized IT security training required for positions such as ISSO, system administrator, and firewall administrator. Ensure that the contractor has a security awareness training program for all employees on the contract.

7) If the work is performed at the contractor's facility using the contractor's equipment, be sure to state C&A requirements for the IT system used and that the Government will conduct site review visits at least annually to verify that policies and procedures are being followed.

See TD P 71-10 for further guidance on non-IT contractual security requirements.

Refer to the following NIST documents for further guidance:

- NIST SP 800-4A, *Security Considerations in Federal Information Technology Procurements*
- NIST SP 800-35, *Guide to IT Security Services*
- NIST SP 800-36, *Guide to Selecting IT Security Products*.

3.3 PERFORMANCE MEASURES AND METRICS

The Government Performance and Results Act of 1993 requires agencies to prepare an annual performance plan. For each program activity, agencies are to provide measurable, objective performance goals and performance indicators to measure performance against these goals. These performance indicators are termed "performance measures."

3.3.1 Performance Measures

OMB has defined a set of performance measures for the IT security program. These performance measures are reported annually in accordance with FISMA. In addition, Treasury has defined a performance measure that is reported annually in Treasury's performance report.

The following paragraphs describe these performance measures.

a. **Standards**

1) OMB mandated that the government agencies shall—

Provide a report to OMB on their performance measures on September 15 of each year. The measures often request data from both the current fiscal year (FY) and the previous fiscal year (last FY) to provide a basis for comparison. For example, the report due in September 2003 would request data from FY02 and FY03.

a) Identify the agency's total security funding as found in the agency's current FY budget request, current FY budget enacted, and the President's next FY budget. This funding should include a breakdown of security costs by each major operating division or bureau and include CIP costs that apply to the

protection of government operations and assets.[1] Agencies should exclude funding for CIP pertaining to lead agency responsibilities such as outreach to industry and the public.[2]

b) Identify and describe as necessary the total number of programs and systems in the agency and the total number of systems and programs reviewed by the Program Officials, CIOs, or Inspectors General (IG) in last year's report and in this year's report according to the format provided below. Agencies should specify whether they used the NIST self-assessment guide or an agency-developed methodology. If they used the latter, they should confirm that all NIST guide elements were addressed.

Programs and Systems	Previous FY	Current FY
a. Total number of agency programs.		
b. Total number of agency systems.		
c. Total number of programs reviewed.		
d. Total number of systems reviewed.		

c) Identify all material weakness in policies, procedures, or practices, as identified and required to be reported under existing law. Identify the number of reported material weaknesses for last FY and this FY, and the number of repeat weaknesses in this FY.

Material Weaknesses	Previous FY	Current FY
a. Number of material weaknesses reported.		
b. Number of material weaknesses reported in previous fiscal year.		

d) Identify and describe any specific steps taken by the agency head to clearly and unambiguously set forth FISMA's responsibilities and authorities for the agency CIO and Program Officials. Specifically, how are such steps implemented and enforced? Can a major operating component of the agency make an IT investment decision without review by and concurrence of the agency CIO?

e) How does the agency head ensure that the agency's information security plan is practiced throughout the life cycle of each agency system? During the reporting period, did the agency head take any specific and direct actions to oversee the performance of agency Program Officials and the CIO to verify that officials such as these are ensuring that security plans are up to date and practiced throughout the life cycle of each system?

[1] Agencies should report security costs that agree with those reported on their current year and next year Exhibit 53s. If security costs detailed in an agency's Exhibit 53 were incomplete or inaccurate, corrected security costs should be reported. Differences with the final current year Exhibit 53 also should be noted with the agency's next year Exhibit 53.

[2] The following agencies have lead agency responsibilities pertaining to CIP: Commerce, Treasury, Environmental Protection Agency, Transportation, Federal Emergency Management Agency, Health and Human Services, Energy, Justice, State, Department of Defense, and Central Intelligence Agency.

f) How has the agency integrated its information and IT security program with its CIP responsibilities and other security programs (e.g., continuity of operations, and physical and operational security)? Does the agency have separate staffs devoted to other security programs and are such programs under the authority of different agency officials? If so, what specific efforts has the agency head or other officials taken to eliminate unnecessary duplication of overhead costs and to ensure that policies and procedures are consistent and complementary across the various programs and disciplines?

g) Has the agency undergone a Project Matrix[3] review? If so, describe the steps the agency has taken as a result of the review. If not, describe how the agency identifies its critical operations and assets, interdependencies, and interrelationships, and how the agency secures those operations and assets.

h) How does the agency head ensure that the agency, including all components, has documented procedures for reporting security incidents and sharing information regarding common vulnerabilities? Identify and describe the procedures for external reporting to law enforcement authorities and to the General Services Administration's (GSA) Federal Computer Incident Response Center (FedCIRC). Identify actual performance according to the measures and the number of incidents reported in the format provided below.

Incident Response	No.
a. Total number of agency components, including bureaus and field activities.	
b. Number of agency components with incident handling and response capability.	
c. Number of agency components that report to FedCIRC.	
d. Does the agency and its major components share incident information with FedCIRC in a timely manner consistent with FedCIRC and OMB guidance?	
e. What is the required average time to report to the agency and FedCIRC following an incident?	
f. How does the agency, including the programs within major components, confirm that patches have been tested and installed in a timely manner?	

	Previous FY	Current FY
a. By agency and individual component, number of incidents (e.g., successful and unsuccessful network penetrations, root or user account compromises, DoS attacks, Web site defacing attacks, malicious code and virus, probes and scans, and password access) reported by each component.		

3 Project Matrix is a program developed by the Department of Commerce's CIAO to identify and characterize accurately the assets and associated infrastructure dependencies and interdependencies that the U.S. Government requires to fulfill its most critical responsibilities to the nation. OMB directed most large agencies to undergo a Project Matrix review.

	Previous FY	Current FY
b. By agency and individual component, number of incidents reported externally to FedCIRC or law enforcement.		

In responding to the performance measures below, include the number of systems reviewed, the total number of systems, and the resulting percentage (e.g., 98/102, 96 percent).

i) Have agency Program Officials 1) assessed the risk to operations and assets under their control, 2) determined the level of security appropriate to protect such operations and assets, 3) maintained an up-to-date security plan (that is practiced throughout the system life cycle) for each system supporting the operations and assets under their control, and 4) tested and evaluated security controls and techniques?

Component or Bureau Name	Total Number of Systems
Total Number of Agency Systems	

By each major agency component and aggregated into an agency total, from last year's report and this reporting period, identify the actual performance according to the measures and format provided below for the number and percentage of total systems.

Component or Bureau Name				
	Prev. FY #	Prev. FY %	Curr. FY #	Curr. FY %
a. Systems that have been assessed for risk.				
b. Systems that have been assigned a risk level after a risk assessment has been conducted (e.g., high, medium, or basic).				
c. Systems that have an up-to-date security plan.				
d. Systems that have been authorized for processing following C&A.				
e. Systems that are operating without written authorization (including the absence of C&A, expired or never performed).				
f. Systems that have the costs of their security controls integrated into the system's life cycle.				

Component or Bureau Name				
g. Systems for which security controls have been tested and evaluated in the past year.				
h. Systems that have a contingency plan.				
i. Systems for which contingency plans have been tested in past year.				
Agency Total				

j) For operations and assets under their control, have agency Program Officials used appropriate methods (e.g., audits or inspections) to ensure that contractor-provided services (e.g., network or Web site operations) or services provided by another agency for their program and systems are adequately secure and meet the requirements of FISMA, OMB policy and NIST guidance, national security policy, and agency policy? Identify actual performance according to the measures and in the format provided below.

Component or Bureau Name		
	Previous FY	**Current FY**
a. Number of contractor operations or facilities.		
b. Number of contractor operations or facilities reviewed.		

In this section, the agency must respond to performance measures and provide narrative responses where appropriate to identify and describe the performance of agency CIOs in fulfilling their security responsibilities. For each category, include the number of systems reviewed, the total number of systems, and the resulting percentage (e.g., 98/102, 96 percent).

k) Has the agency CIO 1) adequately maintained an agencywide security program, 2) ensured the effective implementation of the program and evaluated the performance of major agency components, and 3) ensured the training of agency employees with significant security responsibilities? Identify the actual performance according to the measures and in the format provided below.

	Prev. FY	**Curr. FY**
a. Other than GAO or IG audits and reviews, how many agency components and field activities received security reviews?		
b. What percentage of components and field activities have had such reviews?		
c. Number of agency employees, including contractors.		
d. Number and percentage of agency employees, including contractors, who received security training.		
e. Number of employees with significant security responsibilities.		
f. Number of employees with significant security responsibilities who received specialized training.		

	Prev. FY	Curr. FY
g. Briefly describe what types of security training were available.		
h. Total costs for providing the training described in (g).		

Training	Y/N
a. Do agency POA&Ms account for all known agency security weaknesses, including all components and field activities? If not, why not?	
b. Has the CIO appointed a senior agency information security official?	

l) For operations and assets under his or her control (e.g., network operations), has the agency CIO used appropriate methods (e.g., audits or inspections) to ensure that contractor-provided services (e.g., network or Web site operations) or services provided by another agency are adequately secure and meet the requirements of FISMA, OMB policy and NIST guidance, national security policy, and agency policy? Identify actual performance according to the measures and in the format provided below. (See FISMA Sections 3532(b)(2), 3533(b)(2), and 3534(a)(1)(B) and (b)(1))

	Previous FY	Current FY
a. Number of contractor operations or facilities.		
b. Number of contractor operations or facilities reviewed.		

m) Has the agency CIO fully integrated security into the agency's capital planning and investment control process? Were security requirements and costs reported on every capital asset plan (and Exhibit 53) submitted by the agency to OMB? If not, why not? Identify actual performance according to the measures and in the format provided below.

	Current Year +1 Budget Materials	Current Year +2 Budget Materials
a. Number of capital asset plans and justifications submitted to OMB.		
b. Number of capital asset plans and justifications submitted to OMB without requisite security information and costs.		
c. Were security costs reported for all agency systems on the agency's Exhibit 53?		
d. Have all discrepancies been corrected?		
e. How many capital assets has the CIO or other appropriate official independently validated before submittal to OMB?		

2) Treasury mandated that the bureaus shall provide reports on the following performance measure:

This performance measure is reported annually in Treasury's annual performance report. E-ITSPA collects the data semiannually from the bureaus. Activity: Treasury-wide Management Policies and Program.

Function: Develop and implement policies relative to the internal management of the Department and its bureaus and to coinage and currency production and security.

Measure: Percentage of Treasury IT systems that are currently certified and accredited to operate.

Definition: Per OMB Circular A-130, Appendix III, all major applications and general support IT systems must be certified and accredited following appropriate departmental or agency IT security guidelines. The percentage is determined by dividing the number of systems certified and accredited by the total number of systems in operation.

Validation: Data will be collected and maintained by Treasury's DASIS/CIO/E-ITSPA office. E-ITSPA will conduct a survey semiannually. Departmental senior management will review the survey and the resulting data. E-ITSPA staff will verify data during annual compliance reviews.

b. **Procedures**

OMB issues an annual data call for the data required for the annual FISMA report. E-ITSPA is tasked with collecting data from the bureaus, validating the data received, and preparing a report for OMB for the DASIS/CIO. Throughout the year, bureau Program Officials and bureau CIOs are responsible for collecting the data required in the above performance measures. The bureau CIO is specifically tasked by DASIS/CIO with providing the report to E-ITSPA.

E-ITSPA will issue semiannual data calls through the DASIS/CIO for the Treasury performance measure. The final numbers for the Treasury performance measure will be provided to the Treasury CFO in October of each year for the annual performance report.

3.3.2 Metrics

IT security metrics are tools designed to facilitate decisionmaking, performance, and accountability through collection, analysis, and reporting of relevant performance-related data. The purpose of measuring performance is to monitor the status of measured activities and facilitate improvement in those activities by applying corrective actions, based on observed measurements. To provide meaningful data, quantifiable security metrics must be not only based on IT security performance goals and objectives but also easily obtainable and feasible to

measure. Security metrics must be repeatable, show relevant performance trends over time, and be useful for tracking performance and directing resources.

a. **Standards**

Program Officials and bureau CIOs shall establish at least five internal security metrics to track the progress of their IT security programs.

b. **Procedures**

NIST SP 800-55, *Security Metrics Guide for IT Systems*, describes the process for designing and for sample metrics.

3.4 CRITICAL INFRASTRUCTURE PROTECTION

The CIP initiative is concerned with providing and maintaining adequate levels of security and redundancy to ensure the performance of a minimal set of government and human-related services vital to the protection of people, the stability of the national economy, and the security of the nation. The TCI is a combination of critical national Treasury functions; associated personnel; and supporting IT systems, emergency preparedness communications, and physical assets/facilities.

PDD-63, *Critical Infrastructure Protection*, dated May 1998, stipulated that the national goal is to ensure that any interruptions or manipulations of these critical national infrastructures are brief, infrequent, manageable, geographically isolated, and minimally detrimental to the welfare of the United States.

a. **Standards**

1) Bureaus shall be responsible for funding and conducting Project Matrix initiative interdependency analyses of their critical functions and services and for reporting these results to E-ITSPA. E-ITSPA will coordinate and schedule the steps of the initiative with the bureau and perform the work with the CIAO and/or the Treasury team. The first iteration will be comprehensive followed by updates to each step based on guidance by the CIAO or as significant changes to the information functions and services occur.

2) Bureaus shall be responsible for conducting vulnerability assessments of their IT critical assets at least annually. Bureaus shall document any weaknesses found in their POA&M.

3) A centralized asset management system shall be established for CIP information assets and maintained by E-ITSPA.

4) Bureaus shall establish and maintain a bureau program for the protection and assurance of the critical infrastructure. The bureau program shall incorporate the capital planning and investment processes, life-cycle management, and architecture planning; integrate with existing security program efforts; maximize the performance of resources, including measurable outcomes; and not be duplicative.

b. **Procedures**

1) A Treasury-wide process should be established and maintained to identify and prioritize critical infrastructure, interdependent and dependent relationships, protection concerns, and protection solutions. The process shall include a centralized reporting system for critical asset management.

2) Vital records necessary to ensure continuity of operations and to protect the legal and financial rights of the Department and persons affected by the Department shall be protected.

3) Necessary public and private sector partnerships should be established as a means of reducing shared risk and coordinating TCI requirements.

3.5 SYSTEM DEVELOPMENT LIFE CYCLE

Like other aspects of information processing systems, security is most effective and efficient if planned and managed throughout an IT system's life cycle, from initial planning; through design, implementation, and operation; to disposal. Many security-relevant events and analyses occur during a system's life.

The principal reason for implementing security during a system's development is that it is more difficult to implement it later (as is usually reflected in the higher costs of such later implementation). Later implementation also tends to disrupt ongoing operations.

The five basic phases of a computer system's life cycle are as follows:

- **Initiation.** During this phase, the need for a system is expressed and the purpose of the system is documented.
- **Development and Acquisition.** During this phase, the system is designed, purchased, programmed, developed, or otherwise constructed. This phase also may include other defined cycles, such as the system development cycle or the acquisition cycle.
- **Implementation.** After the initial system testing, the system is installed or fielded.
- **Operations and Maintenance.** During this phase, the system performs its work. The system is usually modified by the addition of hardware, software, and numerous other events.
- **Disposal.** The computer system is disposed of once the transition to a new computer system is completed.

Each phase can apply to an entire system, a new component or module, or a system upgrade. The IT system life cycle itself is only one component of other life cycles (for example, the information life cycle). Information (e.g., personnel data) is used much longer than the life of one computer system.

a. **Standards**

An initial risk assessment shall be performed during the initiation phase to determine risks. An initial system security plan (SSP) shall be drafted detailing the security requirements of the system. These security requirements shall be incorporated into the system requirements and, like all other system requirements, tracked, updated, and validated throughout the system life cycle.

b. **Procedures**

Refer to TD P 84-01, *Information System Life Cycle Manual*, which may be obtained through the Treasury intranet.

3.6 SECURITY CHANGE MANAGEMENT

The IT infrastructure at Treasury is expanding and continually becoming more complex. There are more people depending on the network, more client machines, upgraded and expanded administrative systems, and more application programs. As the interdependency between the IT infrastructures grows, a strong change management process becomes essential. From time to time, each IT element requires downtime for planned upgrades, maintenance, or fine-tuning. In addition, unplanned outages may occur that may result in upgrades, maintenance, or fine-tuning. Managing these changes is a critical part of providing a robust and valuable IT infrastructure.

After a baseline requirements document is developed and approved, the configuration management plan for the IT system is invoked. Change is inevitable as the developing organization responds to the needs of the user and new technology developments. All changes must be assessed for impact on the IT system components and their cost and schedule. The impact of a change on the security posture of the IT system should also be assessed as part of the configuration management process because changes may adversely affect the overall security posture of the infrastructure and the IT system.

a. **Standards**

1) Bureaus shall evaluate the impact on the security posture for all proposed changes to an IT system, including security patches.

2) The ISSO for an IT system shall be a voting member on the CRB for the IT system.

3) The ISSM shall be a voting member on the bureau CCB for the bureau's IT architecture.

4) A formal written change request shall be submitted to the CRB for all changes, scheduled and unscheduled. The change request shall be assigned to the appropriate personnel, including the ISSO, to determine the impact of the change on the IT system and its interdependencies, including the security posture of the IT system (or its supporting general support system). If the change request creates a major change in the security posture of the system, the C&A of the IT system shall be updated.

5) All changes shall be tested and evaluated before implementation.

b. **Procedures**

Procedures for evaluating, approving, and installing security patches should be in place to ensure that these patches are installed in a timely manner and in conformance with the configuration management plan. (Exploits of vulnerabilities are often available less than a month after the vulnerability is announced.)

3.7 RISK MANAGEMENT

An effective risk management process is an important component of a successful IT security program. The principal goal of an organization's risk management process should be to protect the organization and its ability to perform its mission—not just its IT assets.

Risk is the net negative impact of the exercise of a vulnerability, considering the probability and impact of the occurrence. Risk management is the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level.

a. **Standards**

1) Program Officials shall ensure that risk assessments for the general support and major application systems supporting their program are developed and updated. Risk assessments should be performed whenever there is a major change to the IT system or, if there have been no major changes, every 3 years.

2) The DAA shall determine, based on the analysis provided by the ISSO, whether to accept a risk or to implement countermeasures. The acceptance or rejection of the risk and the justification for the decision shall be documented in the risk assessment report.

b. **Procedures**

Acceptance of low-risk items is not usually a difficult decision. DAAs should be cautious in accepting medium- and high-risk items, considering not only the cost of the countermeasures but also the cost to the agency if the vulnerability were to be exploited. The cost to the agency includes quantifiable items (e.g., recovery costs and lost productivity) and nonquantifiable items (e.g., trust and reputation). DAAs, as senior officials, are accountable to the Secretary for the residual risks they accept. Acceptance of high risk should be rare. ISSOs need to present their risk analysis to the DAA in business terms—namely, the impact on the mission (e.g., cost, schedule, productivity, trust, and reputation).

The overall risk level of a system can be determined using Table 3-2.

Table 3-2. Example of Proposal to Determine Risk Levels

RISK LEVEL			
Criteria	**High Risk**	**Moderate Risk**	**Low Risk**
National critical asset	Yes	N/A	N/A
Enterprisewide system	Yes	N/A	N/A
Confidentiality, integrity, and availability	If any of the three is rated high	If none is rated high but any is rated medium	If all three are rated low

Refer to NIST SP 800-30, *Risk Management Guide for IT Systems*, for further guidance on risk management.

3.8 CERTIFICATION AND ACCREDITATION

C&A is *the* critical IT security process. It requires the risk-managed, cost-effective application of federal and Treasury IT security policies, standards, and procedures. It also demands senior management involvement in the decisions affecting the security of mission data and IT resources. These are the reasons E-ITSPA chose "the number of IT systems certified and accredited" as the performance measure for Treasury's IT security program.

The following paragraphs describe the C&A process as it relates to the life-cycle management of the IT system and define the standards and procedures for certification and for accreditation.

3.8.1 Certification and Accreditation and Life-Cycle Management

The C&A process does not start after quality assurance (QA) testing and just before implementation. It starts at system initiation, during the development of the business case to obtain funding for the system, and it continues throughout the system life cycle.

Business cases must address both the IT and the security resources projected to be required for the new IT system. To assist in determining the security resources required, an initial rough cut risk assessment is conducted to identify the countermeasures that would need to be implemented for the system. This effort requires the Program Official to define, in general terms, the confidentiality, integrity, and availability requirements for the system because these elements determine the system's sensitivity and level of risk.

After the Program Official has obtained funding for the system, the development and acquisition phase begins. The initial risk assessment is refined. At this point, the DAA decides which risks to accept. The risk assessment documents this decision. The SSP (or System Security Authorization Agreement [SSAA] if one is using the NIACAP) provides the system's security requirements. These requirements are incorporated into the system's requirements document and are then tracked throughout the development process (as are all requirements). The requirements are documented in, for example, system design, database design, program specifications, and user and operator manuals. They also are included in the design reviews. Security requirements are documented in designs of interfaces with other bureau systems and in interconnection

agreements for other systems; both types of documents should be approved by the DAAs of the systems involved. When a baseline is established, the configuration management plan is invoked. For each change to the baseline, the impact on the security features of the system is assessed. The effectiveness of the security controls is tested as part of the QA process. At the end of the testing, the SSP (or SSAA) is updated and a final risk assessment is conducted. The ST&E report provides the results of the security testing. The final risk assessment details the residual risk.

The certifier reviews the final SSP (or SSAA), risk assessment, and ST&E report. The certifier then prepares a statement for the DAA recommending the type of accreditation: full, interim, or disapproved. The certifier briefs the DAA on the accreditation package and the justification for the certifier's recommendation. The DAA makes the final decision regarding the type of accreditation, signing the document prepared by the certifier to document this decision.

If the system receives a full or interim accreditation, the management portions of the security plan are implemented (such as training the users on the security features and rules of behavior for the system, periodic testing of the contingency plan, or periodic vulnerability testing). If accreditation is denied, the system cannot be placed into operation until the weaknesses have been corrected, tested, documented, certified, and accredited by the DAA.

The risk assessment and SSP (or SSAA) are updated as changes occur in the system or environment throughout the system life cycle. The C&A is updated whenever a major change occurs, or every 3 years, whichever comes first.

Throughout the life cycle, IT security is an integral part of the multidisciplinary team developing and maintaining the system.

3.8.2 Certification and Accreditation Management Issues

This section details the management procedures needed for C&A.

a. **Standards**

1) Appoint the certifier. Bureau heads shall appoint certification officials in writing.

2) Appoint the DAA in writing.

a) **Enterprisewide IT.** The DAA shall be the Assistant Secretary whose program the IT system supports.

b) **Bureau IT.** Bureau heads shall designate, to the extent it is considered appropriate, Deputy Assistant Secretary/Assistant Commissioner or equivalent level officials as DAAs for their respective offices. Where an IT system substantially involves more than one DAA, one shall be designated the DAA by mutual agreement.

c) **Interconnection Agreements.** Agreements shall be established with all agencies in accordance with NIST SP 800-47. For systems in which the DAA is not the CIO, the coordination should include a CIO signoff.

3) **Inventory.** The bureau ISSM shall maintain an inventory of major applications and general support systems. This inventory shall contain, at a minimum, the system name, platform, and type (major application or general support); its interfaces and interconnections; whether it is an IT critical asset; and the dates for the last vulnerability test, risk assessment, and C&A.

b. **Procedures**

1) Bureaus should establish procedures for the coordination of the accreditation package.

2) Bureaus should establish records retention schedules for accreditation packages. Bureaus may wish to retain the previous accreditation package. The bureau ISSM shall retain the official file copy of all accreditation packages. The storage container used shall be appropriate for the highest sensitivity of information that will be stored in the container. At a minimum, it shall be a locked file cabinet.

3.8.3 Certification

Certification consists of a technical evaluation of a sensitive application or network to determine how well it meets its security requirements. There are five steps in the process:

- **Planning.** Planning involves performing a quick, high-level review of the entire system.
- **Data Collection.** Critical information that shall be collected includes system security requirements; risk analysis data showing threats and assets; system flow diagrams showing not only inputs, processing steps, and outputs but also transaction flows for important transaction types; and a listing of application system controls.
- **Basis Evaluation.** A basis evaluation has four tasks:
  - Risk analysis to understand the security problem by identifying security risks, determining their magnitude, and identifying areas needing safeguards
  - Validation, verification, and testing, in which validation determines the correctness of a system, verification checks for internal consistency, and testing uses data to examine system behavior
  - Security safeguard evaluation to assess the security solution through use of aids such as checklists, control matrices, and weighted ratings for levels of security produced by different controls
  - IT audit to assess whether controls satisfy management's control objectives; the audit uses the same aids used in security safeguard evaluation.
- **Detailed Evaluation.** In the application areas, one analyzes the quality of the security safeguards from one or more of the following points of view:
  - Functional operation controls function property
  - Performance controls satisfy performance criteria
  - Penetration resistance controls that can be easily broken or circumvented.
- **Report of Findings.** The report contains technical and management security recommendations.

a. **Standards**

The certification package shall consist, at a minimum, of the following:

1) Final risk assessment

2) SSP

3) ST&E report

4) Certification statement recommending the type of accreditation and the justification for the type of accreditation.

(**Note:** The SSAA under the NIACAP contains all this information.)

b. **Procedures**

The certifier should ensure that ST&E testing validates the technical and nontechnical controls. Examples of documents the certifier may want to review are the Rules of Behavior, configuration management plan, contingency plans, test plans and test procedures used, interface control documents, and interconnection agreements. The certifier may incorporate these documents into the accreditation package kept on file.

3.8.4 Accreditation

Accreditation is a policy decision by management resulting in a formal declaration that appropriate security countermeasures have been implemented properly for the IT system activity so that the activity is operating at an acceptable level of risk. The DAA uses the certification report to help evaluate certification evidence. The DAA decides on the acceptability of application security safeguards, approves corrective actions, ensures that corrective actions are implemented, and issues the accreditation statement. The authorization and approval for an IT system to process sensitive data in an operational environment are granted on the basis of a certification by designated technical personnel that the design and implementation of the system meet prespecified technical requirements for achieving adequate security. Accreditation is official management authorization to operate.

a. **Standards**

1) The DAA shall grant one of three types of accreditation: full, interim, or denied.

a) **Full Accreditation.** Full accreditation shall be granted when—

- The certification package described in Section 3.8.3 is complete
- No corrective actions are required
- Residual risks are acceptable to the DAA.

b) **Interim Authority to Operate (IATO).** The following documentation, at a minimum, shall be provided for an IATO:

- Risk assessment
- An SSP

- A POA&M schedule for correcting the deficiencies to achieve full accreditation. This plan must be mutually acceptable to the Program Official and the DAA.

c) **Denied.** If the system cannot meet IATO requirements or the residual risks are considered by the DAA to be too high to accept, the accreditation shall be denied. The system may not be placed into operation until at least an IATO can be granted.

2) The accreditation package shall consist of the certification package and the accreditation decision letter.

3) Limitations in resources and technical capabilities may prevent full compliance with the satisfaction of all security requirements without introducing unacceptable delay in achieving the operational requirements the IT system was intended to satisfy. In this section, an "exception" indicates that the implementation of one or more security requirements is postponed temporarily and that satisfactory substitutes for the requirement(s) may be used for a specified time period. The DAA is authorized to grant exceptions to some security requirements identified in the Treasury IT Security Program under the following conditions:

a) The request shall include a statement of the requirements that are to be excepted and for what duration, evidence stating why the identified requirements cannot be implemented, and the offsetting countermeasures that are to be substituted.

b) The request for an exception shall also state what aspect of the threat is related to the proposed request and shall submit evidence that the consequent risk to the system and to the sensitive information it processes, stores, or transmits will be acceptable based on other countermeasures that will be employed over the specified period.

c) A plan for implementing the excepted security requirements later in the life cycle shall be developed.

d) Approval of the exception shall make it incumbent on the DAA to take the necessary programmatic, planning, and funding steps to ensure implementation of any security requirements that are postponed temporarily as a consequence of approval of the exception.

e) The approved written exception shall be maintained with the accreditation package.

b. **Procedures**

1) Four typical cases in which IATO will be employed are as follows:

a) A new system is in an advanced test phase and must use some actual operational data for final design and test before initial operational capability.

b) A survey has concluded that there are no apparent security problems that would allow unauthorized persons to access data in a system, but there has

been neither sufficient time nor resources for rigorous hardware and software testing to determine, for example, if need-to-know restrictions are fully implemented.

c) The configuration of an operational system has been altered. Initial security evaluation by appropriate personnel does not reveal any severe problems, but a full evaluation has had scheduling delays.

d) A system that will be fielded at multiple sites has been evaluated in a test environment. Full accreditation will occur at the site when it is installed.

2) Enterprisewide IT may have an architecture in which primary processors are at a specific facility, with subordinate satellite servers for specific functions at bureau locations. The enterprise DAA will accredit the primary processors. The satellite servers will be certified, and the enterprise DAA will accredit the satellite servers with an IATO for a standard configuration at the development laboratory. After the satellite server is installed at the bureau, the certification will be updated to reflect the bureau environment, and the appropriate bureau DAA will accredit the satellite server.

3.9 IT SECURITY REVIEW AND ASSISTANCE PROGRAM

The IT Security Review and Assistance Program has been identified in the Treasury Strategic Plan as contributing to the strategic objective to "Strengthen Treasury's ability to ensure proper and effective oversight of bureau operations."

a. **Standards**

1) Program reviews shall be conducted using NIST SP 800-26, Security Self-Assessment Guide for IT Security Systems. Weaknesses found during these reviews shall be documented in the bureau's POA&M.

2) E-ITSPA shall conduct reviews of at least four bureaus per year.

3) Using the POA&M, E-ITSPA shall track the status of resolution of all weaknesses and shall verify that each weakness is corrected before closing that item on the POA&M.

b. **Procedures**

1) NIST ASSET

NIST has developed the Automated Security Self-Evaluation Tool (ASSET) to assist agencies in performing reviews using NIST SP 800-26.

As described in NIST SP 800-26, the results of the ASSET questionnaire provide a "method of evaluating the security of a particular system or group of systems." Through interpretation of the questionnaire results, users are able to assess the IT security posture for any number of systems within their organization and, in particular, assess the status of the organization's security program plan.

ASSET consists of two tools: ASSET-System and ASSET-Manager. Within ASSET-System, the questionnaire is presented in a progressive format, allowing users to move backward and forward in the questionnaire at their discretion. The ASSET-Manager provides an ability to not only sort and summarize the questionnaire results for all systems assessed but also display the results through several formatted reports or through an export capability.

ASSET-System enables users to return to the assessment of a particular system by saving the prior status of the assessment. Once the assessment is completed, a user can locally generate summary reports of individual systems, giving an immediate picture of the assessment results.

Both ASSET-System and ASSET-Manager are developed and designed to meet the GSA Section 508 accessibility standards, as required by law.

For more information on ASSET, see http://csrc.nist.gov/asset/.

2) E-ITSPA Reviews of Bureau Programs

a) E-ITSPA will review the bureau's comments on the E-ITSPA review report, shall assist the bureau in taking corrective actions and in resolving outstanding systems security issues, and will provide technical guidance and support. If any major outstanding issues remain unresolved, E-ITSPA may report these observations as material weaknesses to the Department's Office of Accounting and Internal Control.

b) E-ITSPA will maintain oversight and contact with the bureau reviewed after the systems security review and issuance of the report. E-ITSPA will conduct an onsite support visit about 1 year after completion of the review to ensure that the bureau has implemented corrective actions and to provide technical assistance and guidance.

3.10 SECURITY WORKING GROUPS AND FORUMS

3.10.1 Information Technology Security Policy Forum

a. **Objectives**

1) Promote organizational relationships and lines of communications as necessary to ensure that Treasury bureaus can carry out departmental IT security responsibilities

2) Serve as a forum for disseminating information pertaining to state-of-the-art technologies and methods for securing IT systems.

b. **Standards**

A representative from each bureau shall attend every meeting. Representatives shall disseminate the information provided at the meeting to persons who have an appropriate clearance and a need to know within their bureau.

c. **Procedures**

1) Bureau representatives to the IT Security Policy Forum should be designated in writing by proper authority within 30 days of receipt of this policy. A letter of designation should be sent to the Director, E-ITSPA. Replacement representatives should be designated as soon as possible, but no more than 30 days after the departure of the representative.

2) Multiple representations are authorized to appropriately address telecommunications and applications disciplines.

3) The IT Security Policy Forum should meet at least quarterly.

4) E-ITSPA should arrange for at least one classified threat briefing each year.

5) E-ITSPA should notify bureau CIOs when their bureaus are not represented at the meeting.

3.10.2 Treasury Infrastructure Protection Panel

a. **Objectives**

1) Participate in the Treasury-wide CIP Program

2) The Executive Steering Committee will oversee Treasury CIP Program implementation activity.

b. **Procedures**

Each bureau CIAO should attend the meetings. Meetings will be held quarterly. The bureau CIAO for all bureaus with CIP functions and services should attend this meeting.

3.10.3 Information Technology Security Training Forum

a. **Objectives**

1) Promote collaboration on IT security training efforts throughout the Department in support of the departmentwide and bureau IT security awareness and training programs

2) Share information regarding bureau-developed training activities, methods, and tools to save costs and avoid duplication.

b. **Procedures**

1) Bureaus should appoint members to this forum who are responsible for the IT security training and awareness program within the bureau.

2) Meetings should be held at least quarterly.

3.10.4 CIP Working Group

a. **Objectives**

1) Develop policy, strategic and implementation plans, and guidance to ensure that Treasury bureaus are able to carry out compliance programs and compliance responsibilities

2) Coordinate the activities of the Treasury Cyber CIP Program.

b. **Standards**

A representative from each bureau that has CIP assets shall attend every meeting. Representatives shall disseminate the information provided at the meeting to persons who have an appropriate clearance and a need to know within their bureau.

c. **Procedures**

1) Meetings should be held quarterly or as needed. Participation is mandatory for bureaus with CIP functions and services and optional for bureaus with no CIP functions.

2) E-ITSPA should notify bureau CIOs when their bureau is not represented at the meeting.

3.10.5 Compliance Working Group

a. **Objectives**

1) Promote organizational relationships and lines of communications necessary to ensure that Treasury bureaus are able to carry out compliance programs and compliance responsibilities

2) Serve as a forum for the dissemination of information pertaining to FISMA requirements and for methods of developing compliance programs within each bureau.

b. **Standards**

A representative from each bureau shall attend every meeting. Representatives shall disseminate the information provided at the meeting to persons who have an appropriate clearance and a need to know within their bureau.

c. **Procedures**

1) Bureau representatives to the Compliance Working Group should be designated in writing by proper authority within 30 days of receipt of this policy. A letter of designation should be sent to the Director, E-ITSPA. Replacement representatives should be designated as soon as possible, but no more than 30 days after the departure of the representative.

2) The Compliance Working Group should meet at least quarterly.

3) E-ITSPA should notify bureau CIOs when their bureau is not represented at the meeting.

3.11 DISCIPLINARY ACTION

a. **Standards**

1) Bureaus shall establish procedures for disciplinary actions for security violations for employees, in accordance with applicable personnel and conduct regulations. These disciplinary actions shall take into account the sensitivity of the information involved and the number of prior offenses. Security awareness training and the Rules of Behavior for each system shall specify the disciplinary actions for security violations.

2) Bureaus shall adopt standard contract terms, consistent with the Federal Acquisition Regulations, which shall be incorporated into all contracts that permit contractor employees access to these systems that provide similar procedures for contractor employees. These contract terms shall also permit the Government to exclude contractor employees from accessing these systems.

3) Suspected security violations shall be reported to the OIG (TIGTA for the Internal Revenue Service) for investigation and recommended disciplinary action.

b. **Procedures**

1) For employees, remedial action may range from the following actions:

   a) Reassignment of work duties

   b) Disqualification from a particular assignment

   c) Letter of warning

   d) Suspension

   e) Removal.

2) Contractors committing security violations should be removed from the contract.

3) Depending on the security violation, criminal sanctions may also apply.

4) Consult with the appropriate bureau employee relations office and labor relations office in preparing the disciplinary action procedures for employees. Consult with the Contracting Officer for security violations involving contractors.

4. OPERATIONAL CONTROLS

4.1 PERSONNEL

4.1.1 Background Investigations

All individuals accessing sensitive IT systems in the Federal Government require some level of background investigation, the type of which is determined by the sensitivity of the position. Knowledge of the duties that a particular position will require is necessary for determining the sensitivity designation of the position. Various sensitivity designations are assigned to positions in the Federal Government. Determination of the appropriate designation is based on such factors as the type and degree of harm (e.g., disclosure of private information, interruption of critical processing, and computer fraud) the individual could cause through misuse of the computer system and more traditional factors, such as access to classified information and fiduciary responsibilities. It is important to select the appropriate position sensitivity because controls in excess of the sensitivity of the position waste resources, whereas insufficient controls might result in unacceptable risks.

a. **Standards**

1) Program Officials and bureau heads shall ensure that adequate funding is available for the required background investigations for employees and contractors accessing their sensitive IT systems.

2) All employees and contractors accessing sensitive IT systems are subject to a security background investigation that is appropriate to the sensitivity of the position.

3) Employees and contractors shall not access sensitive IT systems until they have a favorably adjudicated National Agency Check.

b. **Procedures**

1) First, determine the risk level for the IT systems the contractor or employee should access (see Table 3-2 under Risk Management). Table 4-1 provides examples of recommended minimum security background investigations based on the risk level. Consult with your bureau's personnel security officer to determine the appropriate position sensitivity level and background investigation for employees and contractors.

The MBI (Minimum Background Investigation) is used for individuals in positions designated as low risk. The BI (Background Investigation) is used for individuals in positions designated as moderate risk. The Single Scope Background Investigation (SSBI) is used for individuals in positions designated as high risk.

Table 4-1. Examples of Minimum Background Investigations

Position	High Risk	Moderate Risk	Low Risk
DASIS/CIO	SSBI	N/A	N/A
Bureau CIO	SSBI	N/A	N/A

Position	High Risk	Moderate Risk	Low Risk
CIPO/CIAO	SSBI	N/A	N/A
DAA	SSBI	BI	MBI
ISSM	SSBI	BI	MBI
ISSO	SSBI	BI	MBI
System Administrator	SSBI	BI	MBI
Security Administrator	SSBI	BI	MBI
Database Administrator	SSBI	BI	MBI
Network Administrator	SSBI	BI	MBI
Developer	SSBI	BI	MBI
Field Engineer	SSBI	BI	MBI

2) Certain positions may require access to national security information. The incumbents of these positions need a clearance appropriate to the level of classified information they must access. For example, the bureau representatives to the IT Security Policy Forum must have a Secret clearance. Senior managers typically are required to have a Top Secret clearance.

   See TD P 71-10 for additional information.

4.1.2 Rules of Behavior

OMB Circular A-130 requires all major applications and general support systems to have Rules of Behavior. These Rules of Behavior are part of a comprehensive program to provide complete information security. These guidelines are established to hold users accountable for their actions and responsible for IT security. Rules of Behavior delineate responsibilities and expected behavior of all individuals with access to the system in recognition of the fact that knowledgeable users are the foundation of a successful security program.

a. **Standards**

1) Bureaus shall establish Rules of Behavior for each general support system and major application in coordination with the bureau's Chief Counsel.

2) All users of Treasury IT systems shall be trained in the Rules of Behavior for the systems to which they are granted access before receiving access.

3) All users shall sign a statement acknowledging that they have received and understand the training.

4) Any failure to comply with the Rules of Behavior shall be considered a security incident. If the incident is deemed willful, it will be escalated to a security violation and may be subject to disciplinary actions.

b. **Procedures**

The statement acknowledging the Rules of Behavior training should be filed in either the employee's official personnel file (OPF) or the employee personnel file (EPF) maintained by the office. Coordinate with your human resources office on the appropriate record system to use to file these forms. The signed statement should be retained until the user either resigns or transfers outside of Treasury.

Refer to NIST SP 800-18 for examples of Rules of Behavior.

4.1.3 Access to Sensitive Information

Sensitive information is information that requires protection from unauthorized disclosure, loss, misuse, or unauthorized access or modification that could adversely affect the interest or conduct of federal programs, or the privacy to which individuals are entitled under the Privacy Act, but that has not been specifically authorized under criteria established by an act or Executive order to be kept secret.

Poor or inadequate access control over a user's files or documents may permit information to be copied or modified by unauthorized persons or to become corrupted unintentionally or maliciously. Access control is the way to protect the user's information and data files.

a. **Standards**

1) Access to information and documents shall be carefully controlled to ensure that only authorized personnel have access to sensitive information.

2) Access to sensitive information shall be given to employees who have a validated need to know.

b. **Procedures**

Develop either a form or an automated system for granting access to IT systems, whereby management within the organization must authorize access.

4.1.4 Separation of Duties

Although the organization of each department is unique, IT responsibilities should be distributed among several individuals. This separation is necessary for adequate internal control of the IT system. This process refers to dividing roles and responsibilities so that a single individual cannot subvert a critical process.

a. **Standards**

Bureaus shall establish, document, and enforce procedures to ensure separation of duties for sensitive IT systems.

b. **Procedures**

The following are examples of separation of duties.

1) **Financial System.** One individual should be responsible for the accounts receivable; another, for the accounts payable.

2) **Network System.** One individual should be responsible for backing up the system; another, for the physical access controls; and another, for the privileges.

4.1.5 Training and Awareness

An IT security awareness and training program enhances security by improving awareness of the need to protect system resources; developing skills and knowledge so that computer users can perform their jobs more securely; and building in-depth knowledge to design, implement, or operate security programs for systems. The program also supports individual accountability.

a. **Standards**

1) Bureaus shall develop, fund, and implement a security awareness and training program and plan for all employees who are involved in the development, management, use, or operation of sensitive IT systems.

2) Bureaus shall ensure, through appropriate contractual provisions, that contractor employees involved in the development, management, use, or operation of sensitive IT systems receive security awareness training commensurate with their duties.

3) Bureau's IT security awareness and training programs shall include specialized training for all personnel with significant security responsibilities. Specialized training may be developed in-house or purchased. Personnel with significant security responsibilities include the following functions and shall be provided with specialized "targeted" training (titles may vary from bureau to bureau): senior executives/Program Officials, ISSMs, ISSOs, system administrators, DAAs, and systems certifiers.

4) Bureaus shall establish and maintain a means of tracking training program management information, such as training costs and numbers of personnel trained. Bureaus' records regarding numbers trained shall include, at a minimum, the number of personnel receiving general security awareness and the number of personnel receiving specialized training.

5) Summary information regarding the bureau's security awareness and training program shall be reported in accordance with the instructions contained in Treasury's annual data call issued in support of FISMA.

6) Bureaus shall provide initial training before system access is granted, and within 30 days of appointment for new personnel who are managers, users, or operators of sensitive IT systems.

b. **Procedures**

1) Bureaus should provide continuing training whenever a significant change occurs in the bureau or office environment or procedures.

2) Bureaus should provide annual refresher training for all personnel responsible for the management, use, or operation of sensitive IT systems. E-mail messages, newsletters, memorandums, curriculum materials, and videos are examples of acceptable methods for refresher awareness training.

3) IT security awareness and training plans reflect the overall and specific security training goals for the year and should contain, at a minimum, the following information:

   a) IT security awareness and training content or subject matter (i.e., security basics, security planning and management).

   b) Target audience, including bureau and contractor personnel, for each of the training content areas.

   c) Level of training (i.e., awareness or specialized) to be provided for each specific subject matter area and target audience category.

   d) Information pertaining to the bureau-established Rules of Behavior.

   e) IT Security Training Program costs refer to all information systems security training and awareness training costs. Costs shall include how much is spent on training products for development or purchase; how much is spent on managing training, such as scheduling, booking, planning, and traveling to attend training; and how much is spent on "opportunity costs," such as time spent in training or employee time. Specialized training costs may be found in bureau offices of human resources, which often centrally maintain records of employee training.

4) Treasury recommends the establishment of certification programs for IT security professionals. A professional certification establishes a consistent method for assessing personnel skills and competency. An agency with certified personnel on staff operates at a known level of professional competency.

4.1.6 Separation From Duty

Effective administration of users' computer access is essential to maintaining system security. User account management focuses on identification, authentication, and access authorizations. Considerations involve the timely modification or removal of access and associated issues for employees who are reassigned, promoted, terminated, or retired, or have access revoked for other causes. Similar issues arise for contractors and detailees. Procedures for managing accounts are important in preventing unauthorized access to your system.

a. **Standards**

1) All appropriate personnel shall be notified promptly of all reassignments, promotions, terminations, or retirements of departing employees or contractors to ensure that accesses are removed.

2) Access shall be suspended for any employee or contractor on extended leave or detail over 90 days. Supervisor or Contracting Officer's Technical Representative must request reinstatement of access upon the return to active duty of the employee or contractor.

3) Bureaus shall implement procedures that require departing employees to return all media used to gain system access on their last workday.

4) All accounts shall be deactivated within 1 day of an individual's departure on friendly terms and immediately upon an individual's departure on unfriendly terms.

5) An exit interview shall take place to ensure that all areas are covered before the individual departs.

b. **Procedures**

1) Bureaus should ensure that all official data and e-mail are transferred to the supervisor for review.

2) Bureaus should ensure that the equipment is properly reformatted/cleared to be reused.

4.2 PHYSICAL SECURITY POLICIES

4.2.1 General Physical Access

General physical access controls restrict the entry and exit of personnel from an area, such as office building, data center, or room containing IT equipment. These controls protect against threats associated with the physical environment.

It is important to review the effectiveness of general physical access controls in each area during business hours and at other times. Effectiveness depends on not only the characteristics of the control devices used but also the implementation and operation.

a. **Standards**

1) Bureaus shall establish access controls to ensure that only authorized persons have access to Treasury or bureau buildings and structures housing sensitive IT equipment.

2) Visitors to a facility shall sign in and shall be escorted the entire time they are in the facility.

3) Combinations or entry codes shall be changed at least annually or whenever a person who knows the combination departs or no longer requires access.

b. **Procedures**

1) Bureaus should limit access to those individuals who need access through the use of guards, identification badges, or entry devices (e.g., key cards).

2) Bureaus should consider alarms and exterior lighting for those facilities located in a high crime area.

3) Bureaus should consider physical protection measures for those areas that house power transformers or distribution panels.

4) Bureaus should safeguard all unissued keys or other entry devices.

5) Bureaus should establish procedures to retrieve identification badges, key cards, keys, etc., when employees or contractors depart or no longer need access.

4.2.2 Sensitive Facility Access

The physical protection of IT and telecommunications switches and any connected remote terminals is a prime concern to the successful operations of Treasury functions. Physical protection requirements should meet the minimum standards established for any category of restricted-access data. In addition, IT and telecommunications switch facilities need to be afforded adequate protection from all unauthorized personnel.

a. **Standards**

1) Bureaus shall establish and maintain an access roster for all limited-access rooms or facilities, such as data centers, LAN rooms, or telecommunications closets. The access roster shall be reviewed at least annually.

2) Personnel not on the access roster for a limited-access room or facility shall sign in and out and shall be escorted the entire time they are in the room or facility. The ISSO shall maintain these sign-in logs for 1 year.

3) Combinations or entry codes shall be changed at least annually or whenever a person who knows the combination departs or no longer requires access.

b. **Procedures**

1) Bureaus should limit access to those individuals who need access through the use of guards, identification badges, or entry devices (e.g., key cards, combination locks, keys).

2) Bureaus should safeguard all unissued keys or other entry devices.

3) Bureaus should establish procedures to retrieve keys and entry devices when employees or contractors depart or no longer need access.

4.3 MEDIA CONTROLS

4.3.1 Media Protection

In the use of removable storage media, additional information security risks are associated with the portability of the media. Information security issues to be considered are as follows: a) loss or disappearance of disks or other storage media can compromise the confidentiality, integrity, or availability of the organization data; and b) damage to the media compromises the integrity of records.

a. **Standards**

1) All media shall be marked with the appropriate sensitivity level and kept in a limited-access location onsite. Backup and archive media shall be sent to a offsite location having appropriate security controls, as identified through the contingency plans.

2) Records shall be established to track all deposits and withdrawals from media storage facilities and libraries.

3) Bureaus shall maintain an accurate record of the media's chain of custody and hold users accountable for the media removed from storage.

4) Records shall be secured to prevent unauthorized access and manipulation of log information.

5) Bureaus shall maintain records of receipt of disks or other storage media that are transferred to another location by courier or mail.

b. **Procedures**

Bureaus should establish procedures for access, storage, and transportation of all media containing sensitive information. These procedures should address logs for depositing and withdrawing media from onsite storage facilities and libraries, and backup storage facilities and procedures for the proper wrapping and labeling of media to be mailed or couriered.

See TD P 71-10 for additional guidance.

4.3.2 Media Marking

a. **Standards**

1) If a bureau requires markings other than limited official use (LOU), bureaus shall establish sensitivity levels and the associated labels, in accordance to TD P 71-10.

2) LOU media shall be stored and marked in accordance to TD P 71-10. Bureaus shall establish storage, mailing, and marking procedures for each level of sensitivity they define.

4.3.3 Sanitization

NCSC-TG-025, *A Guide to Understanding Data Remanence in Automated Information Systems*, provides information regarding data remanance and the procedures that can be used to ensure that data cannot be recovered from electronic media. The guide may be obtained from the Superintendent of Documents, U.S. Government Printing Office, Washington, DC 20402.

a. **Standards**

1) Sanitization methods shall be commensurate with the sensitivity of the data residing on storage devices or equipment.

2) All magnetic media, diskettes, hard disks, or other storage devices containing sensitive data or software shall be sanitized before the transfer, reuse, surplus, or donation of any equipment or media.

3) Removable or portable media that are to be reused within the same department shall be used after reformatting.

4) Contracts with external companies for repair or recovery of data from systems, hard drives, or media shall require a nondisclosure statement, in accordance with TD P 71-10.

5) Before being disposed of, any device containing a hard drive or memory that has processed sensitive information shall be cleaned by commercial disk-wiping software or by degaussing the hard drive and all chips containing memory. A letter stipulating that this procedure has been complied with shall be signed by the security person who has performed this procedure and must accompany the device when it is turned into property management for disposal.

b. **Procedures**

Table 4-2 lists suggested methods for clearing or sanitizing various types of media.

Table 4-2. Clearing and Sanitization Matrix

Media	Clear Before Reuse	Sanitize Before Disposal or Surplus
Magnetic Tape1		
Type I	a or b	a, b, or m
Type II	a or b	b or m
Type III	a or b	m
Magnetic Disk		
Bernoullis	a, b, or c	m
Floppies	a, b, or c	m
Nonremovable Rigid Disk	c	a, b, d, or m
Removable Rigid Disk	a, b, or c	a, b, d, or m
Optical Disk		
Read Many, Write Many	c	m
Read Only		m, n
Write-Once, Read-Many (WORM)		m, n
Memory		
Dynamic Random Access Memory (DRAM)	c or g	c, g, or m
Electronically Alterable PROM (EAPROM)	i	j or m
Electronically Erasable PROM (EEPROM)	i	h or m
Erasable Programmable ROM (EPROM)	k	l, then c, or m
Flash EPROM (FEPROM)	i	c then i, or m
Programmable ROM (PROM)	c	m
Magnetic Bubble Memory	c	a, b, c, or m
Magnetic Core Memory	c	a, b, e, or m
Magnetic Plated Wire	c	c and f, or m
Magnetic Resistive Memory	c	m
Nonvolatile RAM (NOVRAM)	c or g	c, g, or m
Read Only Memory (ROM)		m
Static Random Access Memory (SRAM)	c or g	c and f, g, or m
Equipment		
Cathode Ray Tube (CRT)	g	q
Printers		
Impact	g	p then g
Laser	g	o then g

a. Degauss with a Type I degausser.
b. Degauss with a Type II degausser.

c. Overwrite all addressable locations with a single character.
d. Overwrite all addressable locations with a character, its complement, and then a random character, and verify.
e. Overwrite all addressable locations with a character, its complement, and then a random character.
f. Each overwrite must reside in memory for a period longer than the classified data resided.
g. Remove all power, including battery power.
h. Overwrite all locations with a random pattern, all locations with binary zeros, all locations with binary ones.
i. Perform a full chip erase as per manufacturer's data sheets.
j. Perform i above, then c above, a total of three times.
k. Perform an ultraviolet erase according to manufacturer's recommendation.
l. Perform k above, but increase time by a factor of three.
m. Destroy—disintegrate, incinerate, pulverize, shred, or melt.
n. Perform the destruction required only if classified information is contained.
o. Run five pages of unclassified text (font test acceptable).
p. Destroy ribbons and clean platens.
q. Inspect and/or test screen surface for evidence of burned-in information. If burned-in information is present, a CRT must be destroyed.

4.3.4 Production and Input/Output Controls

a. **Standards**

Bureaus shall establish procedures to ensure that media, including tapes, disks, and paper, are not accessed by unauthorized individuals.

b. **Procedures**

The following are examples of procedures that should be used to protect output:

1) Obtain physical bins to place printouts from high-speed printers and from facsimile (fax) machines.

2) Enable banner settings for all print jobs.

3) Use certified mail when mailing sensitive information.

4) Require users to be at the printer when they are printing sensitive information.

4.3.5 Disposal

a. **Standards**

1) All equipment with hard drives shall be sanitized before being placed on surplus.

2) Portable electronic devices (PED) shall be destroyed.

3) Sensitive media shall be sanitized or destroyed.

b. **Procedures**

See Table 4-2 above for clearing and sanitizing methods.

4.4 VOICE COMMUNICATIONS

4.4.1 Private Branch Exchange

These guidelines and procedures help minimize the risk of unauthorized access and unauthorized usage of digital private branch exchanges (PBX) within Treasury and aid in reducing vulnerabilities inherent in such systems.

a. **Standards**

1) Bureaus shall restrict access to PBX equipment to authorized personnel only.

2) Bureaus shall disable (if possible) or monitor remote access ports.

b. **Procedures**

Refer to NIST SP 800-24, *PBX Vulnerability Analysis: Finding Holes in Your PBX Before Someone Else Does*, for procedures for analyzing the vulnerabilities in your PBX and to implement countermeasures for them.

4.4.2 Telephone Communications

Most Treasury desk telephones are unsecure. Very few persons have secure telephone equipment as their desk telephone. Treasury personnel and contractors shall be trained to be careful about what information is being discussed over an unsecure telephone and to recognize attempts to obtain sensitive information, including passwords and access codes.

a. **Standards**

Bureau policy regarding the sensitivity of its information shall include whether the information can be communicated over an unsecure telephone or fax or whether secure telephone equipment shall be used.

b. **Procedures**

Bureaus should train their personnel on what sensitive information may be discussed over unsecure telephones and what sensitive information must be discussed using secure telephone equipment. Personnel should also be trained to recognize social engineering attempts.

4.4.3 Voice Mail

a. **Procedures**

To reduce exposure to risk associated with telecommunications systems, voice mail messages should be retrieved by the use of a password chosen by the employee. Individual voice mail passwords should be treated as any other password; they should neither be shared with anyone nor posted to or around a telephone device. Passwords should be changed at least every 90 days.

4.5 DATA COMMUNICATIONS

4.5.1 Telecommunications Protection Techniques

a. **Standards**

1) The Department of the Treasury shall protect all telecommunications transmissions for all sensitive information by the most cost-effective means possible. An example of an effective means of protecting telecommunications is end-to-end encryption.

2) Bureaus shall select the telecommunications protection techniques that meet their security needs, consistent with departmental and bureau security policies, in the most cost-effective manner possible.

4.5.2 Facsimile

Fax technology was developed for scanning and transmitting documents or pages. The term "fax" is derived from a patent application filed in 1885. Although fax is traditionally a telephony-based application, the technology has evolved to address the transmission of text or image files. Standards are under development for Internet-based fax using store-and-forward protocols and real-time connectivity between Internet Protocol (IP) connected fax gateways.

Fax is an inherently insecure means of communication that can be easily intercepted and decoded. Fax protocols provide neither authentication nor nonrepudiation services; therefore, fax traffic can be sent to or received by improper recipients. The commonly used Group III fax protocol implements support for proprietary and undocumented data exchange using a feature called nonstandard facilities (NSF). Fax servers or fax modems attached to networks provide a potential means of network intrusion and penetration.

a. **Standards**

1) Implement appropriate fax security measures for all sensitive information. If sensitive material is faxed over public communication lines, one of the following methods shall be used:

a) An authorized staff member is present at the time of transmission to properly handle the materials at the receiving site.

b) The fax is sent to a locked room to which only authorized personnel have access.

c) A password-protected fax mailbox is used to restrict release to an authorized individual.

2) Sensitive information shall not be faxed to untrusted intermediaries (e.g., hotel staff or convention centers).

3) **Fax Servers, Gateways, Modems, and Boards**

a) Place fax servers and gateways that connect a Treasury IP network to an external IP network (e.g., the Internet) on extranets.

b) Do not directly attach fax modems and boards to networked workstations. Fax modems and boards may be directly attached to stand-alone workstations.

c) Implement discretionary access control (DAC) mechanisms (e.g., password protected in-box) on fax servers and gateways that store sensitive data.

d) Disable and enable remote maintenance (e.g., dial-in) ports for fax servers and gateways only as needed for authorized maintenance or repair.

4) **File Transfer.** Scan binary files received using fax protocols with virus-checking software.

5) **Encryption.** If encryption is used, encrypt sensitive information during receipt and transmission using a National Security Agency (NSA) approved or FIPS 140-1 or FIPS 140-2 compliant method.

b. **Procedures**

1) **Operation and Usage**

a) Bureaus should ensure that accurate phone numbers are used for fax transmissions and that the broadcast lists used to automate the sending of faxes are accurately maintained.

b) Bureaus should monitor, or use password-protected in-boxes for, data received during operational hours on stand-alone fax machines that are used for the receipt of sensitive data. This procedure is not needed for environments that have sufficient physical access controls to prevent unauthorized access to sensitive fax output.

4.5.3 Video Teleconferencing

Video teleconferencing permits Treasury personnel to engage in live exchanges of information without the lost time and high cost of traveling to attend a face-to-face meeting in a distant city. Video teleconferencing offers many beneficial applications, including training and distance learning, data collaboration, large and small meetings, and informational broadcasts.

a. **Standards**

1) Bureaus shall select the telecommunications protection techniques that meet their security needs, consistent with departmental and bureau security policies, in the most cost-effective manner possible.

2) Video conferencing shall be disabled when not in use.

3) Adequate security shall be provided for all sensitive information transmitted in a video teleconference, regardless of form.

b. **Procedures**

1) Bureaus should ensure that all members have a need to know and that nonmembers cannot listen in.

2) Bureaus should ensure that any videotapes created of the teleconference are appropriately labeled and secured based on the sensitivity of the information on the videotape.

4.5.4 Voice over IP

Voice over IP (VoIP) telephony enables the transfer of voice data over a packet-switched network as opposed to the traditional circuit-switched networks of today's telephone companies. Companies are moving to this technology because it allows them to use their existing network infrastructure to carry data and voice traffic. Savings come from eliminating the need to purchase new PBX equipment and from reduced staff and maintenance costs because only one network needs to be supported.

Current voice traffic on circuit-switched networks has a very high level of quality because each connection is guaranteed a certain bandwidth (64 kilobits per second [kbps]) for the life of the call. When voice traffic is transmitted over an IP-based network, the data is compressed to 7.9 kbps or 6.3 kbps, depending on which standard is being used (G.729 or G.723.1). This savings in bandwidth comes at a price in the quality level of the call. On an IP-based network, packets can travel over any number of different routes, so the quality of the transmission is tied to the quality of the network.

As with any technology still in its infancy, various standards are being proposed as the best way to achieve industry acceptance. The following industry standards are in place to deal with current IP telephony implementations:

- H.323 is a comprehensive protocol that tries to address all aspects of a VoIP system. A secure call can be achieved using encryption-based authentication or subscription-based authentication; however, performance may be degraded.
- Session Initiation Protocol (SIP) is a less complicated, and some would argue, more flexible, protocol. It is a challenge-response-based system similar to the Hypertext Transfer Protocol (HTTP).
- Multimedia Gateway Control Protocol (MGCP) systems are composed of Media Gateways, Signaling Gateways, and Media Gateway Controllers. MGCP does not require end-user devices capable of complex processing, as does H.323. MGCP gateways should be able to work with H.323, SIP, and legacy telephones.

a. **Standards**

1) VoIP equipment are computers; therefore, the underlying operating systems shall be configured appropriately just as they are for data servers.

2) Bureaus shall disable microphones on VoIP telephone units.

b. **Procedures**

1) Do not use the same media device for voice and data. Doing so allows hackers to acquire access to all conversations traversing the network.

2) Build redundancy into the VoIP network to allow for the possibility of alternate ways of providing phone service if major network problems occur.

3) Bureaus ensure that firewalls are VoIP aware. Hackers may ride into a network through a firewall by manipulating an H.323 packet.

4.5.5 Communications Circuits

A communication circuit is an electronic physical device that sends information and/or data from one location to another.

a. **Standards**

1) Bureaus shall safeguard all physical telecommunication devices from theft and tampering.

2) Bureaus shall allow only authorized personnel to access or modify any telecommunication device.

4.6 WIRELESS COMMUNICATIONS

4.6.1 Cellular Phones

a. **Standards**

1) Bureaus shall establish policy and train users concerning which topics can and cannot be discussed on unsecure cell phones as a result of the risk of interception of radio signals or being in a public area where conversations can be overheard easily.

2) Sensitive information shall be discussed only on NSA-approved secure cellular equipment.

3) Unsecure cell phones shall not be taken into any area where classified information is discussed.

4) Cell phones with cameras shall not be taken into any area where sensitive or classified information is processed, stored, or discussed.

b. **Procedures**

Bureaus should establish procedures to disable cell phones in areas where sensitive information is discussed and to collect cell phones before entering any area where classified information is discussed.

4.6.2 Wireless Local Area Network

Wireless local area network (WLAN) technology enables one or more devices to communicate without physical connections. WLAN uses radio transmission as a means of transmitting data, whereas wired technology uses cables.

Wireless networks are used as the transport mechanism between and among devices and the traditional wired network. They allow greater flexibility and portability than do traditional wired

LANs. Wireless networks connect computers and other components to the network using an access point device. This device communicates with devices equipped with wireless network adaptors.

a. **Standards**

The following security criteria shall be implemented for WLANs accessing sensitive IT systems:

1) All access to Treasury's sensitive IT systems shall be protected with federal government-approved devices or techniques that provide explicit user I&A and audit trails.

2) Encrypted WLANs shall comply with Section 5.5.1, Encryption, of this handbook.

3) Bureaus that implement wireless networks shall establish monthly vulnerability testing to ensure the WLAN security, including scanning for rogue access points.

b. **Procedures**

Use NIST SP 800-48, *Wireless Network Security, 802.11, Bluetooth and Handheld Devices*, for guidelines regarding securing wireless networks.

4.6.3 Pagers

Two types of text messaging pager systems exist: one-way and two-way. Text pagers can send text messages of from 110 to 160 characters long, depending on the carrier. Text messages also can be sent from a cellular service provider's Web page or by visiting Web sites that allow users to send text messages for free. Text messages rely on the service provider's network and are not encrypted; there are no guarantees on the quality of services. Text message devices can be spammed with text messages until their mailbox is full and the user is no longer able to receive new text messages unless previously stored e-mail is deleted.

a. **Standards**

Two-way pagers shall not be taken into areas where classified information is processed or discussed.

b. **Procedures**

1) Develop a property inventory list of all pagers. This list will include serial numbers and/or seat numbers and user names for accountability purposes.

2) Establish procedures for using two-way pagers. Include whether two-way pagers will be permitted in areas where highly sensitive information is processed or discussed.

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 also can be used to play video games. Most of these functions have no security.

a. **Standards**

A risk assessment shall be conducted on all wireless devices. The assessment shall include the risks associated with all functions, including infrared (IR), radio frequency (RF), and video. The DAA shall know the associated risks that have been identified by the risk assessment. Based on the sensitivity of the data and the associated risk identified by the risk assessment, the DAA shall approve or disapprove the use of multifunctional wireless devices.

b. **Procedures**

1) Develop procedures for removing data before the transfer or disposal of the equipment.

2) Review NIST SP 800-48, Wireless Network Security, 802.11, *Bluetooth and Handheld Devices*, for additional procedures.

3) For devices with IR ports, bureaus should consider covering the IR port with metallic tape to disable communications using this port.

4.7 OVERSEAS COMMUNICATIONS

a. **Standards**

Bureaus shall adhere to procedures provided in 12 FAM 600 and 12 FAM 500 for all overseas communication. 12 FAM 600 can be found at the uniform resource locator (URL) http://www.state.gov/aboutstate/ when the user clicks on “Foreign Affairs Manual.”

b. **Procedures**

Wireless communications are highly vulnerable to interception and monitoring. Treasury employees overseas should be informed of the risks and the appropriate precautions they should follow.

4.8 EQUIPMENT

4.8.1 Workstation

a. **Standards**

1) Only licensed and approved operating systems and applications shall be used on Treasury personal computers (PC) or workstations.

2) All default vendor or factory set administrator accounts and passwords shall be changed before installation or use.

b. **Procedures**

The Department of the Treasury-owned workstations should have an asset tag and should be inventoried with name, location, and use.

4.8.2 Laptop Computer

Laptop computers include a variety of portable computers, frequently given names such as notebooks or notepads by the manufacturer. Laptop computers are vulnerable to theft and the loss of all data contained on them. Many theft rings operating today at airports and other public places target laptops. The loss or theft of government computers places the information contained on them at risk of loss, disclosure, or compromise. The use of laptops in public (e.g., at airports, restaurants, and conferences; on airplanes; and while traveling) presents a significant risk that unauthorized persons can observe the information being processed. Use of a laptop to transmit information through public telecommunications networks also presents vulnerability. To protect sensitive information from these risks and from unauthorized access, manipulation, and destruction, it is necessary to protect the information by encrypting it.

a. **Standards**

1) All Department of the Treasury-owned laptops shall have asset tags and be inventoried with name, location, and use.

2) All Department of the Treasury-owned laptops shall be marked with the appropriate sensitivity level.

3) All laptop cases shall be marked with an asset tag or be engraved with the Department of the Treasury's address and a phone number.

4) Employees shall not take overseas any laptop used for processing sensitive information, without prior approval of the DAA.

5) Employees shall immediately report any incidents of mishandling, tampering, or the loss of a laptop computer to the bureau security office or the Department of the Treasury, Office of Security and Continuity Planning.

6) Before they are disposed of, ensure that all laptop computers that have processed sensitive information are cleaned by commercial disk-wiping software or by degaussing of the hard drive and all chips containing memory. A letter stipulating that this procedure has been complied with shall be signed by the security person who has performed this procedure and shall accompany computers turned into property management for disposal.

7) Use antivirus software and ensure that virus signature files remain current.

b. **Procedures**

1) Develop a property inventory list of all laptops, including serial numbers and/or seat numbers, user names, and location of all laptops at all times, for accountability purposes. The user should sign a receipt assuming responsibility for the laptop computer by serial number. Laptop computers should not be used

by anyone other than the person who signed for it, without a change of accountability.

2) Ensure that users of laptops processing sensitive information sign a Rules of Behavior statement that stipulates that they understand the security measures necessary for protecting that information and that they further understand the policy regarding the use of laptop computers. All laptops should be controlled using bureau property accountability procedures.

3) Users should request tamper-resistant bags for use when taking a laptop overseas.

4) Be sure to password-protect the BIOS.

5) Use a cable lock or a secured docking station to secure the laptop to the desk.

6) Store the laptop when not in use in a lockable cabinet (e.g., overhead bin, file cabinet, vault, or locked room).

7) Back up critical data before going on travel.

8) Never leave a laptop unattended when on travel.

4.8.3 Portable Electronic Device

PEDs are vulnerable to theft and the loss of all data contained on them. The communication technologies in PEDs enable them to upload and download files using their file sharing option, sometimes without the user's knowledge. Many PEDs also contain sound-recording devices that may activate without the user realizing that the recording function has been turned on. These vulnerabilities necessitate that the use of PEDs be controlled and constrained.

a. **Standards**

1) Department of the Treasury-owned PEDs shall have an asset tag and be inventoried with name, location, and use.

2) Use government-owned PEDs to dial up and connect to the network to perform file sharing or to update calendars. Privately owned PEDs are not authorized to process, transmit, or store sensitive information.

3) A risk assessment shall be conducted on all PED devices. The assessment shall include the risks associated with all functions. The DAA shall review the associated risks that have been identified by the risk assessment. Based on the sensitivity of the data and the risk associated with it, as identified by the risk assessment, the DAA shall approve or disapprove the use of PED devices.

b. **Procedures**

1) Develop a property inventory list of all PEDs. This list should include serial numbers and/or seat numbers, user names, and location of the user of all PEDs at all times for accountability purposes.

2) Government-owned PEDs should have all files erased before being reused by another individual or office within the Treasury.

4.8.4 Privately Owned Equipment and Software

a. **Standards**

Bureaus shall ensure that security awareness educates Treasury employees and contractors about this policy.

b. **Procedures**

Bureaus should conduct reviews, at least semiannually, of all equipment and software to ensure that only government-licensed software and equipment is being used and that appropriate waivers signed by the DAA exist for privately owned equipment or software.

4.8.5 Hardware and Software Maintenance

System maintenance requires either physical or logical access to the system. One of the most common methods hackers use to break into systems is through maintenance accounts that still have factory-set or easily guessed passwords. War-dialing techniques will also reveal maintenance ports that are not protected.

a. **Standards**

Maintenance accounts shall have strong passwords, in accordance with Section 5.1.1, Passwords, of this handbook.

1) If at all possible, maintenance shall be approved by the appropriate IT system manager(s). Affected systems shall be backed up before maintenance begins.

2) Changes made to hardware or software during maintenance shall be logged.

3) IT practitioners (e.g., system administrators, vendor technicians) are the only personnel authorized to perform maintenance activities on Treasury hardware or software. Visiting Treasury practitioners shall adhere to the Department of the Treasury's sensitive facility policy.

4) Following IT system upgrades or consolidations, surplus equipment shall be secured until it has been prepared for surplus.

5) Contracts with maintenance vendors shall identify the security requirements.

4.9 CONVERGING TECHNOLOGIES

In the past many devices, such as copier machines and the heating, ventilation, and air-conditioning (HVAC) controls for buildings and computer facilities, were not part of the IT arena. Thus, IT security concerns were not an issue. With the increased dependence on the reliable performance of the massive IT systems and networks that control the basic functions of our infrastructure comes an increased security risk. Therefore, in the future, other devices and services will be integrated into the IT systems.

a. **Standards**

For all equipment containing IT, bureaus shall perform a risk assessment to identify the vulnerabilities before connecting it to the Treasury or bureau network. Appropriate countermeasures shall be addressed before connecting the equipment to the network.

b. **Procedures**

1) Thoroughly test, evaluate, and approve new hardware and software before implementation throughout the organization.

2) Reduce vulnerabilities through testing, applying patches, and eliminating or disabling unnecessary services.

3) Disable all maintenance ports when they are not being used.

4) Change all default passwords and access codes.

4.10 GENERAL IT SECURITY

4.10.1 Security Incident and Violation Handling

The Treasury Computer Security Incident Response Capability (CSIRC) provides a mechanism for receiving and/or disseminating computer security incident information departmentwide and a consistent capability to respond to, and report on, computer security incidents. The Treasury CSIRC functions in accordance with federal policy and regulations: OMB Circular A-130, Appendix III, Security of Federal Automated Information Resources; PDD-63, *Critical Infrastructure Protection*; and FISMA (formerly, the Government Information Security Reform Act [GISRA]). The Treasury CSIRC also provides the following:

- A framework for identifying, handling, managing, responding to, and reporting computer incidents in a timely and expeditious manner.
- A mechanism for disseminating generic and specific computer security incident information to the CIO, the bureau computer security incident response capabilities, and the Treasury Department Office of Enterprise IT Planning and Operations (E-ITPO) to ensure that actions are being taken to minimize the impact of ongoing or potential incidents.
- Governmentwide information sharing of threats, incidents, and trends to support computer security planning and operations.

a. **Standards**

1) The following events are defined as computer security incidents and shall be reported to the Treasury CSIRC:

a) **Malicious Logic Attacks.** These attacks are performed by crackers and hackers in an attempt to gain privileges and/or information, capture passwords, and modify audit logs to hide unauthorized activity. The attempts include the use of active code such as viruses, Trojan horses, worms, and scripts.

b) **Probes and Reconnaissance Scans.** These scans include probing or scanning networks for critical services or security weaknesses. They also include nuisance scans.

c) **Unauthorized Access and Unsuccessful Attempts.** These attempts include all successful unauthorized accesses and suspicious unsuccessful attempts.

d) **DoS Attacks.** These attacks affect the availability of critical resources, such as e-mail servers, Web servers, routers, gateways, and communication infrastructure.

e) **Alterations/Compromises of Information.** These events involve the unauthorized altering of information or the compromise of information.

f) **Adverse Site Mission Impacts.** These events have significant impact on the mission of the site or operations but do not fall into any of the aforementioned categories.

g) **Classified System Incidents.** These events involve either a system used to process national security information, or classified information on any system not certified for that level of classified information.

h) **Loss or Theft of Equipment.** These events must be reported to the Treasury CSIRC to determine the potential compromise of sensitive material. This effort includes the compromise of user accounts and passwords that could allow unauthorized persons to access Treasury computing resources or agents' names or case information that could compromise an investigation or risk the loss of human life. The Treasury CSIRC's emphasis is on the data that was lost or stolen, not on the hardware itself.

i) **Misuse of Resources.** These events include the misuse of a computing or telecommunications system or network.

j) **Domain Name System (DNS) Attacks.** These attacks affect the availability of services or networks.

k) **Root Compromise.** These events compromise the most trusted privileges of the machines on the network.

l) **Web Site Defacements.** These events compromise the integrity and availability of all public Web sites.

2) Examples of adverse events that are *not* usually within the scope of computer security incident response include unplanned outages and acts of nature, such as floods and fires. However, bureaus shall also report these types of incidents to the Treasury CSIRC within the 1-hour time frame. It is important that bureaus notify the Treasury CSIRC when such incidents occur and affect operations; however, bureaus also should address these types of incidents in the component's business continuity procedures or contingency plans.

b. **Procedures**

Section 6 of this handbook provides security incident and violation handling procedures.

4.10.2 Contingency Planning

a. **Standards**

1) An emergency response capability shall be composed of the following components:

   a) An emergency staff with primary and alternate representatives designated for each key position

   b) A viable plan with recovery procedures that can be successfully executed by the emergency staff

   c) One or more alternate operating facilities for recovery of business operations and services (e.g., manufacturing or site-unique operations; information resources)

   d) Saved, retrieved, and usable vital records

   e) A dynamic crisis management structure.

2) The emergency response capability shall encompass methods and techniques that guarantee a high level of readiness and enable implementation in response to any threat with and without warning. The threat spectrum includes localized acts of nature, accidental incidents, technological emergencies, criminal acts, and terrorist attacks using weapons of mass destruction.

3) Continuity planning shall encompass the following:

   a) Essential government functions shall be identified. A recovery time objective shall be established for each function. The recovery time objective is the longest time period for which a function can be disrupted before serious impacts are experienced. During an emergency, essential government functions shall be recovered and reconstituted no later than the recovery time objective; recovery of other functions deemed noncritical shall be deferred.

   b) A recovery strategy and procedures shall be developed for the resumption of each essential government function, including the associated system, data, application, and telecommunications. The procedures shall include instructions for backing up and restoring tasks, a methodology for reconstructing lost data, steps for implementing alternative work methods or emergency operations, steps required for managing and processing work backlog, and synchronizing of files and data. The recovery strategy shall be assessed for sufficiency in meeting the recovery time objective for the essential government function. Departmental offices and bureaus shall acknowledge risk and any associated data loss.

c) Implementation of recovery strategies may permit service degradation, but this should be mitigated. Strategies may make use of internal recovery, commercial recovery centers, or cooperative agreements or may involve a combination of the aforementioned. Implementation of the strategy may be achieved via hot sites, cold sites, mutual internal support, or reciprocal agreements.

d) A schedule shall be developed for ramping up or rapidly resuming each essential government function.

e) A vital records program shall be established and maintained. Vital records shall be identified, duplicated, and stored off premises in a suitable environment located at a safe distance from the office and bureau. Each departmental office and bureau shall be responsible for sending vital records to and retrieving them from the off-premises storage facility using reliable packing methods and transport mechanisms that guarantee delivery and safe storage of vital records. Frequency of shipping shall correlate directly to the recovery objectives of the departmental office and bureau.

f) Guidance for providing physical and information security.

g) Designation of the emergency staff (teams), duties and responsibilities, and procedures for notification and recall of the emergency staff (teams) during duty and nonduty hours.

h) Succession and emergency delegations clearly stating those individuals authorized to act on the behalf of the senior Treasury officials during an emergency.

i) A strategy for communicating with nonemergency staff and rendering assistance to them as required and needed.

j) Guidance for continued and uninterrupted command, control, and leadership of the affected departmental office and/or bureau.

k) A strategy for communicating with employees, visitors, and others (including the media) during an emergency.

l) Procedures for restoring or replacing damaged or destroyed facilities while maintaining operations at the alternate operating facility or facilities.

b. **Procedures**

1) The bureaus should perform contingency plan using a planning cycle that includes the following phases: initiating and managing a multiyear planning process; defining functional requirements (including risk assessment and business impact analysis activities); designing and developing response and recovery strategies; writing the plan; exercising the plan (including corporate awareness and education programs); and maintaining the plan and the associated emergency response capability. This planning cycle permits implementing disaster recovery and business continuity planning in phases; it is iterative; and change management is crucial for ensuring the synchronization of the plan and the emergency response capability with current business operations and services (including any

manufacturing or other site-unique operations, and information resource requirements).

2) The bureaus should develop a plan using an integrated planning approach. An integrated planning approach usually involves forming a team composed of individuals with expertise in IT (voice and data), security, contingency, and facilities. The team works collectively in developing and coordinating plan requirements and components. The plan should be coordinated with other federal, state, and local governments, and with private sector organizations when necessary, not only to ensure that all plans, infrastructures, and capabilities are interoperable, but also to mitigate conflicting lines of authority. Those departmental offices and bureaus having interdependencies should coordinate planning efforts to ensure compatibility within the Department.

3) The plan should address those strategies and procedures for responding to the emergency (including building evacuation), relocating to one or more alternate operating facilities, restoring utilities (voice and data), restoring operations and processing any backlog of work, resuming essential government functions, moving to any interim operating site(s) during the recovery period, and returning to the home site.

Refer to NIST SP 800-34 for additional guidance.

4.10.3 Documentation (Manuals, Network Diagrams)

a. **Standards**

Security features of all systems shall be part of the standard documentation as defined in TD P 84-01, *Information Systems Life Cycle Manual*.

4.10.4 Information Backup

a. **Standards**

Online or offline data storage is subject to FOIA requests, requests from Congress, litigation, or official investigations. Data is considered to be a federal record when it meets the criteria specified in the statute, and must be safeguarded as such.

1) Implement backup procedures for all of the Department of the Treasury IT systems.

2) Backups are to be protected at the highest level of sensitivity and shall be marked with the highest level of sensitivity.

3) Media containing master copies, including vendor media, shall be protected at the same level as the sensitivity of the system and marked.

4) Backups shall be restricted to authorized personnel only.

5) Periodically (at least monthly) verify backup copies by restoring statistical sampling of file(s) to ensure the integrity of the backups.

6) Create backup procedures, including the following:

a) Frequency

b) Retention

c) Archiving, including sending archive media offsite

d) Offsite schedule, including authorized personnel who are authorized to send and receive backup media

e) Logs of backups, including recording errors that might occur

f) Backup schedule

g) Restore software from the original medium, not from backups.

h) Reconfigure the media in accordance to bureau's policy.

5. TECHNICAL CONTROLS

5.1 IDENTIFICATION AND AUTHENTICATION

User I&A is the means of verifying the identity of users before granting access to a requested resource. Authentication counters the threat of masquerading. Users identify themselves to the system and then authenticate their identity by providing a second piece of information that is known only by the individual user or can be produced only by the user. Authentication can be implemented in varying degrees of strength and lays a foundation for other security services, such as access control and audit.

a. **Standards**

1) Implement and enforce unique user I&A techniques for all individuals who access sensitive IT systems and networks based on the level of risk. At a minimum, user identifications (ID) and passwords shall be used.

2) Ensure that each user has a unique I&A. The DAA must approve the requests for group user IDs. Administrator accounts such as root may require more than one individual to have access. The number of individuals having access for a given server must be kept to a minimum.

5.1.1 Passwords

A password is a sequence of characters that can be used for several authentication purposes. Passwords are often used to authenticate the identity of an IT system user and to grant or deny access to private or shared data.

a. **Standards**

1) Passwords are an important aspect of computer security and are the front line of protection for user accounts. Some of the more common uses of passwords are user-level accounts, Web accounts, e-mail accounts, screen saver protection, and voice mail passwords. Listed below are password requirements:

a) Passwords shall be required for all accounts.

b) New users shall change the password the first time they log on.

c) Passwords shall be at least eight characters long.

d) Passwords shall contain a mixture of uppercase and lowercase letters (if technically possible).

e) Passwords shall contain a numeric or special character.

f) Passwords shall not contain any form of the user’s name or ID.

g) Passwords shall expire every 90 days.

h) Password history shall be kept to prevent the reuse of the last three used passwords.

i) Passwords shall not be a word found in a dictionary (even foreign).

j) Passwords shall be neither shared nor kept in plain view.

k) Passwords shall be audited on a regular basis for compliance.

b. **Procedures**

If passwords are to be written down, they should be placed in a sealed envelope and secured in a locked container.

5.2 ACCESS CONTROL

Access controls provide a technical means of controlling what information users can use, the programs they can run, and the modifications they can make. The controls help protect the operating systems and other system software, the integrity and availability of information, and confidential information from being disclosed to unauthorized individuals.

a. **Procedures**

Bureaus should establish procedures for ensuring appropriate access controls for all systems within their organization. Based on the level of investment, the Program Official should approve the access controls.

5.2.1 Automatic Account Lockout

a. **Standards**

1) Bureaus shall limit the number of logon attempts. Systems shall be configured to lock out a user ID after three consecutive failed logon attempts.

2) Once an account is locked out, the account shall be unlocked by a designated system administrator upon positive identification of the user.

3) All logon attempts shall be recorded in an audit log and are subject to review.

5.2.2 Automatic Session Lockout

a. **Standards**

Where possible, systems shall disconnect a user who has been inactive for a period of time to be determined by the bureau.

5.2.3 Warning Banner

a. **Standards**

1) Department of the Treasury computers and IT systems shall display a sign-on warning banner to all users who log on to government computers and systems. This banner shall be displayed before the request for user authentication, where technically practical.

2) The use of government IT systems shall be subject to monitoring and shall be for limited personal use by Treasury personnel. Government IT systems shall be

subject to monitoring. All data contained on the Department of the Treasury systems is considered the property of the U.S. Government, and there can be no expectation of personal privacy on these IT systems.

3) Orientation and security training or awareness programs for employees shall include notification of the use of sign-on warning banners on Treasury systems.

b. **Procedures**

Configure systems to display the required warning banner in accordance with Department of Justice guidance. All warning banners and security and privacy statements should be approved by the bureau Chief Counsel before implementation.

Example of Internal Warning Banner:

The following banner is recommended for all internal (i.e., not publicly accessible) Treasury systems. It was extracted from NIST SP 800-18, *Guidelines for System Security Plans.* It has been approved by the Department of Justice.

****WARNING**WARNING**WARNING****

This is a Department of the Treasury computer system. Department of the Treasury computer systems are provided for the processing of Official U.S. Government information only. All data contained on Department of the Treasury computer systems is owned by the Department of the Treasury and may, for the purpose of protecting the rights and property of the Department of the Treasury, *be monitored, intercepted, recorded, read, copied, or captured in any manner and disclosed in any manner,* by authorized personnel.

THERE IS NO RIGHT OF PRIVACY IN THIS SYSTEM. System personnel may give to law enforcement officials any potential evidence of crime found on Department of the Treasury computer systems.

USE OF THIS SYSTEM BY ANY USER, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES CONSENT TO THIS MONITORING, INTERCEPTION, RECORDING, READING, COPYING, OR CAPTURING AND DISCLOSURE.

****WARNING**WARNING**WARNING****

Example of Public Web Page and Other Banners:

LEGAL NOTICES FOR TREASURY DEPARTMENT PUBLICLY ACCESSIBLE WEB SITES

PRIVACY NOTICE

If you visit our site to read or download information, we collect and store only the following information about you: the name of the domain from which you access the Internet; the date and time you access our site; and the Internet address of the Web site from which you linked directly to our site. We will not obtain personally identifying information about you when you visit our site, unless you voluntarily choose to provide such information to us by E-mail, by completing a comment form, forum registration site, or other on-line form. The Department of the Treasury does not give, sell, or transfer personal information to third parties, unless required by law, such as the Freedom of Information Act.

For site management, information is collected for statistical purposes. Computer software programs are used to create summary statistics about visits to Treasury Web sites, which are used for such purposes as assessing what information is of most and least interest, determining technical design specifications, and identifying system performance or problem areas. No information subject to the Privacy Act, such as name and address, is collected or used for this analysis. Raw data logs are used for no other purposes and are scheduled for regular destruction in accordance with National Archives and Records Administration Guidance.

Except for authorized law enforcement investigations, no other attempts are made to identify individual users or their usage habits.

The Treasury Web sites do not, as a rule, enable "cookies." One or more Treasury bureaus may use cookies. For additional information specific to a Treasury bureau regarding their use and other privacy information, please visit that bureau's Web site.

Generally, individuals are strongly discouraged from sending any personal information, like a social security number, to the Treasury Web master or any Treasury E-mail address. It may be necessary on certain bureau Web sites to collect personally identifiable information (name, E-mail address, social security number, or other unique identifier), but only if specifically and knowingly provided by you. Personally identifying information you provide will be used only for such other purposes as are described at the point of collection by the bureau asking for the information.

NOTICE OF MONITORING

You are entering an Official United States Government System, which may be used only

for authorized purposes. The Government may monitor and audit usage of this system, and all persons are hereby notified that use of this system constitutes consent to such monitoring and auditing.

Unauthorized attempts to upload information and/or change information on these Web sites are strictly prohibited and are subject to prosecution under the Computer Fraud and Abuse Act of 1986 and 18 U.S.C. §§1001 and 1030.

DISCLAIMER OF ENDORSEMENT

The Department of the Treasury does not endorse any commercial product, service, process, or enterprises. Links to other Web sites and references to any commercial product or enterprise are provided solely for the convenience of the user and do not constitute an endorsement or recommendation. The Department of the Treasury assumes no responsibility for the content or operation of other Web sites.

DISCLAIMER OF LIABILITY

The United States Government (including the Department of the Treasury) makes no warranty, express or implied, including the warranties of merchantability and fitness for a particular purpose, and assumes no legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process described or depicted on this Web site and does not represent that its use would not infringe privately owned rights.

COPYRIGHT STATUS

No copyright may be claimed for any work on this Web site that was created or maintained by Federal employee in the course of their duties. Images and text appearing on this Web site may be freely copied. Credit is requested. If copyrighted material appears on the site, or is reached through a link on this site, the copyright holder must be consulted before the material may be reproduced.

OFFICIAL SEAL, NAMES, AND SYMBOLS

Federal law prohibits use of any symbol, emblem, seal, insignia, or badge of any entity of the Department of Treasury (including the Internal Revenue Service) or any colorable imitation of such words, initials, symbols, emblems, or seals in connection with any advertisement, solicitation, business activity, or product where such use could reasonably be interpreted as conveying the false impression that such advertisement, solicitation, business activity, or product is in any manner approved, endorsed, sponsored, or authorized by, or associated with, the Department of the Treasury or any organization within the Department. See 18 U.S.C. §701, 31 U.S.C. §333 and 31 C.F.R. Part 37.

5.3 AUDIT TRAIL

a. **Standards**

1) Audit trails provide a trace of significant events on the application or server. In accordance with bureau's separation of duty policy, audits trails shall be reviewed at least weekly to—

a) Ensure integrity, confidentiality, and availability of information and resources

b) Investigate possible security incidents

c) Monitor user or system activities where appropriate.

b. **Procedures**

1) Bureaus should create audit trails based on the sensitivity of the data. For example, audit trails may be implemented to record all changes to the database.

2) Retention of audit trails depends on the system's sensitivity. Bureaus should establish the retention period for audit logs in coordination with their record manager and Chief Counsel.

5.4 NETWORK SECURITY

5.4.1 Remote Access

All remote users—for example, teleworkers or personnel on business trips—may need to communicate directly with their organizations' systems to receive or send data and updates. Because these users are physically remote, they will often be connecting through public (insecure) networks. This increases the threat of unauthorized access. Remote access control procedures shall provide adequate safeguards through robust I&A and encryption techniques.

a. **Standards**

1) The following security criteria shall be implemented for bureau remote access circuits accessing sensitive IT systems:

a) All remote access to Treasury's sensitive IT systems shall be protected with Federal Government-approved devices or techniques that provide explicit user I&A and audit trails. A dial-back authentication system is not an acceptable alternative to user I&A and audit trails.

b) Encrypted remote access circuits shall comply with Section 5.5.1, Encryption, of this handbook.

c) Bureaus shall use encryption based on a risk assessment, except for wireless, which must use encryption.

b. **Procedures**

1) Ensure that only legitimate users gain access to IT systems and resources.

2) Ensure that users are authorized to perform only functions authorized by their job function.

3) Ensure that the following three key security measures are implemented in protecting IT systems from the threat of intruders' gaining access via remote connections:

   a) Implement a well-administered user I&A (e.g., password, smart card) process.

   b) Ensure that each system's own audit capability is used to monitor system activity with the host to determine system and network usage, identify user difficulties, and uncover intrusion attempts. Routinely review the audit trails to ensure appropriate responses to threats or system and network misuse. Develop and publish requirements for the timely auditing of unauthorized access attempts. Ensure that the audit capability provides a timely visual or audio alarm.

   c) Protect information in transit from disclosure or tampering.

5.4.2 Network Security Monitoring

To maintain operational assurance, bureaus should monitor their networks. Monitoring is an ongoing activity that examines either the system or users for a) vulnerabilities or threats to the network, b) performance, c) verification of network use, and d) compliance with security policies.

a. **Standards**

1) Department of the Treasury IT systems shall be monitored by an authorized individual to the extent permitted by law. This monitoring may include monitoring of e-mail and e-mail transmissions or attachments, traffic analysis, keystroke monitoring, examination of log files, and examination of any or all computer files. Monitoring may be initiated whenever misuse or possible criminal activity is suspected.

2) Department of the Treasury resources and data, user accounts and directories, user files, user e-mail, or other data is subject to review by designated personnel under appropriate circumstances

b. **Procedures**

Bureaus should ensure that any attempt to observe, tamper with, or extract information from the network by an unauthorized person or device can be identified and that appropriate action can be taken to prevent future occurrences (i.e., auditing, intrusion detection).

5.4.3 Network Connectivity

a. **Standard**

Bureaus shall create interconnection agreements in accordance with NIST SP 800-47, *Security Guide for Interconnecting Information Technology Systems*.

b. **Procedures**

1) Ensure that the information transmitted from any point in a network is received at the destination it was intended to reach and nowhere else.

2) Ensure that the information received at any point in a network is identical in content to the data transmitted (i.e., nothing has been added, removed, or changed).

3) Ensure that all network components (e.g., terminals, terminal controllers, modems, nodes, data links, and telecommunication lines) on the bureau's premises are accessible only to employees with authorized access.

4) Ensure that the sender of the information can verify that receipt was by (and only by) the authorized recipient (i.e., nonrepudiation).

5) Ensure that the recipient of information can verify that the person from whom the communication appears to come is actually the person who sent it (i.e., nonrepudiation).

6) Ensure that adequate alternate paths are available for transmitting information from any point in a network to any other point to which data needs to be transmitted.

7) Ensure that an alternate means of communicating critical information has been identified, implemented, and tested in case a failure of the primary and alternate paths occurs.

5.4.4 Firewalls

Firewalls are devices that control the flow of network traffic between networks employing different security postures. By employing firewalls to control connectivity to these areas, an organization can prevent unauthorized access to the respective systems and resources within the most sensitive areas. For the standards and procedures below, a perimeter firewall is a firewall that connects to the public domain, to the Treasury communication system, to another federal agency, or to another Treasury bureau. An internal firewall cannot have any connections outside the bureau.

a. **Standards**

1) All perimeter firewalls shall be treated as a system and shall be certified and accredited in accordance with TD P 85-01 and NIST SP 800-41, *Guidelines on Firewalls and Firewall Policy*.

2) The following minimum technical security standards shall be followed when implementing IP connections on perimeter firewalls. TD P 85-01 does not recommend or specify specific hardware or software products.

a) **Screening Routers.** Screening routers (if used as a firewall component) shall have the capability to filter based on Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) ports as well as IP addresses and incoming network interfaces. It is not recommended that a screening router be the sole segment of a firewall system; rather, it should form a portion of the defense-in-depth posture.

b) **Services.** Only services that are required shall be permitted (to pass through a firewall). For each permitted service, the following information shall be documented: 1) service allowed (including TCP or UDP port number), 2) service description, 3) business case necessitating the service, and 4) internal controls associated with the service.

c) **Inbound Filtering.** Inbound filtering shall be performed to exclude or reject all data packets that have an internal host address (i.e., source address in the local domain). Inbound filtering shall be in accordance with NIST SP 800-41, Section 4.2, Implementing a Firewall Rule set.

d) **Multilayer Firewalls.** Consult the following sources for information on multilayer firewalls: 1) For information on implementing firewalls, NIST SP 800-41, Section 4.4, Firewall Implementation Approach. 2) For information on Open Systems Interconnect (OSI) for network communications, NIST SP 800-41, Section 2.1, General Introduction to Firewall Technology, including Figure 2.1, OSI Communications Stack, and Figure 2.2, OSI Layers Operated on Modern Firewalls.

e) **Logs.** All firewall systems shall enable an audit capability to monitor firewall operation and substantiate investigations of real or perceived violations of local security policies. At a minimum, the logs shall track services that are allowed or denied by the firewall (i.e., IP address of source and destination, date and time, and URL), attempted access to network services, rejected source routed addresses, Internet Control Message Protocol (ICMP) redirects, and any system information the local security officer deems relevant. The firewall syslog and audit logs shall be reviewed daily.

f) **Inbound Services.** Inbound services shall be prohibited unless a valid business case can establish their validity. Inbound services shall provide strong authentication using one-time or session passwords, challenge and response protocols, digital signatures, or encryption. Port protocols shall be blocked in accordance with NIST SP 800-41, Appendix C, Section C.4, Recommendation for Firewall Policy, Table C.1.

Approval to use these services may not be granted unless it can be demonstrated that the selected firewall configuration provides adequate security. Before implementing any of these services, a waiver or exception

shall be requested from the DASIS/CIO DAA for the Treasury Communication System. The CIO of the requesting agency should also grant approval of the waiver for use within his or her bureau.

g) **Firewall Consoles.** All firewall consoles shall be located in a physically secure area and require technical controls equal to or exceeding the minimum security requirements specified in Sections 5.1–5.3 above. Only designated administrator accounts shall be installed on a firewall.

h) **Monitoring.** The firewall system shall provide for a monitoring capability. This capability can be provided as an integral part of the firewall by the provider or through addition of a third-party product. It is desirable that the monitor program provide a scalable response to attacks. The monitoring product shall provide a remote notification capability.

i) **Demilitarized Zone (DMZ)**. A DMZ is a network created by connecting two firewalls. Systems that are externally accessible but need some protections shall be located on DMZ networks. Refer to NIST SP 800-41, Section 3.2, DMZ Networks for additional information.

j) **Exceptions and Waivers.** Exceptions and waivers to this policy and associated standards require a written request submitted to the DASIS/CIO.

b. **Procedures**

1) Approval of an exception to policy must be received from the DASIS before implementation of the waiver. A request should include the following:

a) A description of the exception and waiver

b) The business case necessitating the service

c) An assessment of the risk associated with granting the service

d) Any actions taken to mitigate the residual risks associated with the requested service.

2) Bureaus shall give preference to acquisitions of firewalls that have been evaluated under the Common Criteria based on protection profiles for medium network environments or higher.

5.4.5 Internet Security

The resources, services, and interconnectivity available via the Internet all introduce opportunities and risks in the Department of the Treasury workplace. With the Internet becoming a complex network, security has become more problematic, with break-ins and attacks now so commonplace that they are considered part of conducting business.

a. **Standards**

1) Internet Connections

a) Connectivity between the public Internet and any classified network shall be prohibited.

b) Connections to the Internet shall be implemented using firewalls that are compliant with the standards and procedures Section 5.4.4, above.

c) Treasury services provided via the Internet shall be implemented using extranets and servers that are isolated from Treasury intranets.

d) Treasury firewalls and servers that are accessible from the Internet shall maintain a comprehensive and functional level of operating system security that will limit command-level access to designated administrators. Audit records shall be recorded on tamperproof media or routed to a host that is not accessible from the Internet.

e) Treasury firewalls and servers that are accessible from the Internet shall provide an intrusion detection capability that will provide real-time alerts when an attack or attempt at bypassing system security occurs.

f) Applications using the Internet or other public networks for the transmission of sensitive information shall use virtual private networks, application-level encryption, or another approved means to protect data.

g) User accounts shall not be installed on externally addressable host systems.

h) The following services and protocols shall be disabled on externally addressable host systems: Network File System (NFS), Network Information System (NIS), Remote Procedure Call (RPC), tftp, UDP, boot services, r commands, Routing Information Protocol (RIP) daemon (routed), and ICMP redirects. All unused ports shall be disabled.

2) World Wide Web (WWW) Servers

a) Internet-accessible WWW servers that store nonpublic information shall perform user I&A before allowing access. I&A will be performed in a secure manner not subject to disclosure or playback attacks. Clear text passwords shall not be transmitted across the Internet.

b) The transmission of nonpublic information from a Department server to an Internet user shall be protected using a secure protocol that provides FIPS 140-1 or 140-2 compliant cryptography.

c) WWW servers shall be configured to prevent any administrative login from the Internet.

d) WWW server software shall be kept current with respect to, for example, security-related system patches, modifications, and fixes.

e) WWW servers shall not monitor HTTP ports using an account (user ID) that has system administrator privileges.

f) The implementation and use of Common Gateway Interface (CGI) scripts on WWW servers shall be monitored and controlled. Scripts shall be written in a manner that prevents a user from obtaining command-level access to the server. Scripts shall not use code that allows user data to be passed to a server as a command string. Scripts shall use code that is robust and capable of handling data exception conditions to parse/process user

input. Server Side Includes (SSI) shall be disabled for directories containing scripts.

3) Access to External Internet Sites

a) Stand-alone workstations used to connect to the Internet are exempt from the following provisions if the workstation does not contain sensitive information. These workstations shall not be connected at any time to a Treasury network.

b) HTTP access to external sites shall be accomplished using an HTTP proxy.

c) Active-X controls shall be approved for use on Treasury intranet sites under the following parameters.

- Users are provided with a Web browser (Internet Explorer) that has been configured to use the "trusted site zone." Intranet sites shall be defined in this zone.
- Active-X controls for intranet host systems have been reviewed to ensure that they comply with Microsoft's security guidelines.
- Browsers are configured so as not to permit user modification of the security configuration.

d) The use of Active-X controls from Internet sites shall be prohibited.

e) User access to Java and/or JavaScript shall be approved at the bureau level. Java approval shall be granted with an understanding that hostile Java code is able to—

- Launch a DoS attack against a client browser.
- Obtain system properties from a client system. Java-enabled browsers shall implement a Java security model that prevents a Java applet from reading and writing files on a client system or establishing network connectivity to a site other than the site from which the applet was downloaded.

f) Files obtained from the Internet shall be scanned using Treasury- or bureau-approved software that will detect malicious logic.

g) Only Treasury- and/or bureau-approved software shall be used to access the WWW, and the software shall incorporate all vendor-provided security patches.

4) File Transfer Protocol (FTP) Servers

a) Departmental FTP servers shall be configured to prevent the execution (from the Internet) of uploaded files.

b) Sensitive information shall not be distributed via publicly accessible FTP servers.

c) FTP servers shall be configured to prevent external users from obtaining security-related information from the directory tree.

5) Internet Mail Gateway

a) E-mail traffic between the Internet and internal networks shall be implemented with centrally managed gateways.

b) Proxy applications shall be used to route mail through firewalls.

c) "Mail boxes" shall not be located on application gateways or other devices used to implement a firewall.

b. **Procedures**

1) Use extranets and servers that are isolated from Treasury intranets to provide Treasury services. Connections between extranets and intranets should be implemented using a firewall that is compliant with Treasury policies.

2) Maintain a comprehensive and functional level of operating system security to limit command-level access to designated administrators using Treasury firewalls and servers. Audit records should be recorded on tamperproof media or routed to a host that is not accessible from the Internet.

3) Bureaus should ensure a) that IDSs are installed on Treasury networks and are configured to provide real-time alerts when an attack or attempt at bypassing system security occurs and b) that alerts are sent to the appropriate individuals for response.

5.4.6 Electronic Mail Security

E-mail is the most popular system for exchanging information over any computer network. The e-mail process is divided into two primary components: a) mail servers, which are hosts that deliver, forward, and store mail, and b) clients, which interface with users and allow users to read, compose, send, and store e-mail messages.

E-mail servers are the hosts on any organization's network that are most often targeted by attackers. Attackers are able to develop methods to exploit the technology. E-mail servers also must communicate with untrusted third parties.

E-mail clients have been targeted as an effective means of inserting malicious code into machines and of propagating this code to other machines.

a. **Standards**

1) Department of the Treasury personnel shall comply with the bureau's Rules of Behavior and the Department of the Treasury's Codes of Conduct.

2) By using Department of the Treasury e-mail, Department of the Treasury personnel shall consent to have their e-mail monitored.

3) Any use of Department of the Treasury IT resources, including e-mail, shall be made with the understanding that such use may not be secure, is not private, is not anonymous, and may be subject to disclosure under FOIA.

4) E-mail spamming—sending or forwarding chain letters, other junk e-mail, or inappropriate messages—shall be prohibited.

5) Users shall ensure that e-mail communications are free of viruses through regular screening of incoming e-mail traffic and virus detection updates.

6) E-mail shall be retained as an official record. By the direction of the General Counsel, no e-mail messages shall be deleted or purged from the e-mail server database until further notice. All deleting or purging of e-mail messages shall be approved by the General Counsel.

5.4.7 Privately Owned E-Mail Accounts

Government-provided e-mail is intended primarily for official and authorized purposes. Privately owned e-mail accounts (nongovernment) are employees' personal accounts with their home Internet carrier.

a. **Standards**

1) Non-Treasury accounts shall not be used for any government or official purposes.

2) Automatic forwarding shall not be used to send messages to non-Treasury accounts.

5.4.8 Penetration Testing and Vulnerability Assessment

Penetration testing may identify previously unknown security problems, configuration errors, and needed patches or updates on mission-critical or sensitive IT systems. Proper steps shall be taken to ensure that vulnerabilities discovered during penetration testing are repaired and that any damages possible in the interim are mitigated. Threats identified through penetration testing shall be documented, and the information passed on to the ISSO and appropriate application managers. Findings that cannot be resolved immediately shall be recorded on the bureau's POA&M.

a. **Standards**

1) Major applications and general support systems shall be tested at least annually or as significant changes are made to the IT system(s).

2) Where interconnected IT systems are present, analyses shall be conducted at least semiannually to identify security threats to the agency through shared system boundaries.

3) All penetration testing shall be coordinated with the Treasury CSIRC.

4) The Treasury CSIRC shall report all penetration testing to FedCIRC.

b. **Procedures**

1) Rules of engagement should be prepared and approved for all penetration testing.

2) If a contractor performs the penetration testing, a qualified government employee should supervise the test.

5.5 CRYPTOGRAPHY

5.5.1 Encryption

Encryption, which is a mathematics-based branch on the transformation of data, deals with the transformation of ordinary text (plaintext) into coded form (ciphertext) by encryption and the transformation of ciphertext into plaintext by decryption. It relies on two basic components: an algorithm (or cryptographic methodology) and a key. The algorithm is the mathematical function used for encryption or decryption, and the key is the parameter used in the transformation.

a. **Standards**

Bureaus shall submit an encryption plan to E-ITSPA for approval before implementation.

b. **Procedures**

1) The encryption plan should include the following:

a) A configuration layout showing complete end-to-end details of the telecommunications or IT systems requiring encryption.

b) The type of encryption to be used.

c) The source of key generation.

d) A strategy for implementing secure voice and data that provides consistent information protection against the threat.

e) If applicable, a key management plan for handling and safeguarding the keying material in support of the encryption. This plan should include the following:

- The sensitivity of the information to be communicated
- The cryptoperiod required
- Key loading method
- Key distribution method (e.g., over-the-air rekeying [OTAR])
- Destruction method.

2) Refer to NIST SP 800-21, *Guideline for Implementing Cryptography in the Federal Government*, for additional procedures and guidance.

5.5.2 Public Key Infrastructure

PKI is a combination of software, encryption techniques, and services that enables enterprises to protect the security of their communications and business transactions on networks. PKI integrates digital certificates, public key cryptography, and certification authority (or authorities) (CA) into a complete enterprisewide network security architecture.

a. **Standards**

1) General

a) **Interoperability.** Treasury shall implement X.509 v3 certificates and use CA components that support version 1 of the NIST *Minimum Interoperability Specifications for PKI Components* as a basis for interoperation between PKI components and various vendors.

b) **Network Connectivity.** CA servers and workstations shall not be connected to or accessible from a non-Treasury network. CA servers and workstations shall be attached to a Treasury LAN or WAN, if protected by a dedicated firewall that is located between the LAN/WAN and the CA servers/workstations. An acceptable firewall shall consist of a screening router, dual-homed host, or another device that can control access at the network and transmission protocol layers. This firewall shall be configured to allow only a minimal set of inbound and outbound services as required for CA operation.

This requirement is not applicable to directory servers used to publish certificates and/or Certificate Revocation Lists.

c) **Certificate Types and Assurance Levels.** Treasury CAs shall support two certificate types (confidentiality and signature) with four levels of assurance (Level 1, Level 2, Level 3, and Level 4). Certificate type and assurance levels shall correspond to the Federal Bridge CA assurance levels of rudimentary (Level 1), basic (Level 2), medium (Level 3), and high (Level 4) and associated X.509 object identifiers defined by the Federal Bridge CA.

The reliance a bureau chooses to place on a given level of certificate assurance shall be based on 1) the amount and type of inherent risk of an activity, 2) the consequence of failure, and 3) the use of risk mitigation controls.

d) **CA Public Key Distribution.** CA public keys used for certificate verification shall be distributed to users in a secure “out-of-band” manner (i.e., via a secure channel other than that used to access a certificate directory).

e) **Meaningful Names.** Subscriber names, as contained within a certificate, shall be unique and meaningful, and shall avoid duplication.

f) **Certificate Expiration**. Certificates shall not have an infinite lifetime and shall be subject to expiration.

g) **CA Archive.** CAs shall maintain an archive of records sufficient to establish the validity of any certificate, including those revoked or expired. Archived records shall be maintained for a period to be determined by CAs in compliance with regulation and records management guidance.

h) **Certificate Policy.** Administrative policy shall be developed for CA management of certificates, consistent with the Internet Engineering Task

Force (IETF) Public Key Infrastructure X.509 (PKIX) RFC 2527, Certificate Policy and Certification Practice Statement Framework

i) **Certification Practice Statement (CPS).** CAs shall operate under a CPS that meets the minimum assurance standards. The CPS shall be consistent with the X.509 standard and conform to IETF PKIX Part IV format.

2) Assurance Levels

a) **Physical Security**

- Level 1 and Level 2
  - When not in use, CA tokens, removable cryptographic modules, and any activation information used to access or enable cryptographic modules, shall be placed in high security locked containers (e.g., with Medeco deadbolt locks, Schlage, or USCAN).
  - CA servers, workstations, and other components shall be located in an environment that prevents unauthorized access to equipment and records.
- Level 3 and Level 4
  - When not in use, CA tokens, removable cryptographic modules, and any activation information used to access or enable cryptographic modules shall be placed in GSA-approved Class VI security containers.
  - CA servers, workstations, and other components shall be located in an environment that prevents unauthorized access to equipment and records and that is protected with intrusion alarms.

b) **CPS.** All CAs shall operate under a CPS that provides a description of—

- How keys and certificates are generated, disseminated, stored, revoked, archived, and managed
- How users identify themselves to a CA
- Operational procedures, including system backup, recovery, and audit
- Physical, procedural, and personnel security controls
- Any third-party reviews or audits
- Incident and security response procedures (which must address the termination or compromise of a CA/registration authority [RA] key).

c) **CA Archive.** CAs shall maintain an archive of records sufficient to establish the validity of any certificate, including those revoked or expired. At a minimum, the following shall be maintained:

- Certificate requests
- Revocation requests
- Active certificates
- Expired certificates.

d) **User Identification**

- Level 1. Users shall apply online and need only supply a valid e-mail address.
- Level 2. Users may be identified online via, for example, a personal identification number (PIN), or secret information. User-supplied ID information shall be protected using the Secure Sockets Layer protocol with 128-bit encryption or an alternative approved by the Treasury Policy Management Authority (PMA).
- Level 3. Users shall present, in person, a photo ID to a CA or an RA. The RA or CA must vet the information presented.
- Level 4. Users shall present, in person, two forms of photo ID, one of which must be Treasury issued, to a CA or an RA. The RA or CA must vet the information presented.

e) **Key Generation and Storage.** Signing keys shall be generated by subscribers. Keys shall be generated and stored using media and cryptographic modules as follows.

- Level 1: N/A
- Level 2:
  - Subscriber key pairs shall be generated and stored using FIPS 140-1 Security Level 1 or higher cryptographic modules.
  - CA key pairs shall be generated and stored using FIPS 140-1 or 140-2 Security Level 2 or higher cryptographic modules.
- Level 3:
  - Subscriber key pairs shall be generated and stored using FIPS 140-1 or 140-2 Security Level 2 or higher cryptographic modules.
  - CA key pairs shall be generated and stored using FIPS 140-1 or 140-2 Security Level 2 or higher cryptographic modules.
- Level 4:
  - Subscriber key pairs shall be generated and stored using FIPS 140-1 or 140-2 Security Level 2 or higher cryptographic modules.
  - CA key pairs shall be generated and stored using FIPS 140-1 or 140-2 Security Level 3 or higher cryptographic modules.

f) **Certificate Revocation.** A certificate shall be revoked if the associated private key is compromised; management requests revocation; or the certificate is no longer needed. The CA shall publish a Certificate Revocation List documenting the revocation of a certificate and identifying the reason for revocation within the time specified below:

- Level 1: No revocation required
- Level 2: Within 6 hours
- Level 3: Within 2 hours
- Level 4: Within 30 minutes.

g) **Audit Requirements**

- Level 1: N/A
- Level 2: CAs shall maintain a system audit trail that records, at a minimum:
  - Configuration changes to hardware or software
  - Operational events (e.g., system startup, system shutdown, and system backup)
  - System access (logon, logoff)
  - Issuance and revocation of certificates
  - Security violations (failed login, network probe/attack).
- Level 3: Same as Level 2 except CAs shall record audit data on Write-Once, Read-Many (WORM) media
- Level 4: Same as Level 3.

h) **Environmental Controls**

- Level 1: N/A
- Level 2 through Level 4:
  - CA media shall be stored in a manner that provides protection from accidental water, fire, or electromagnetic damage.
  - CA backup media and copies of audit logs and archival files shall be maintained in a secure offsite location.
  - System backup sufficient to recover CA and directory service operations shall be performed on a periodic schedule that is described in the CA CPS.
  - Provisions shall be made to protect CA and directory service operation from fire and water damage.
  - CA and directory service operations shall have adequate power, HVAC as required to maintain a reliable operating environment.
  - CA and directory services operations shall be provided with an uninterruptible power supply (UPS) with at least a capability to provide an orderly shutdown in the event of a power failure.
  - Production CA and directory service operations shall develop and test a continuity of operations plan.

i) **Personnel Security**

- Level 1: N/A
- Level 2: CA and RA shall have an MBI (Minimum Background Investigation) using Standard Form 86, “Questionnaire for National Security Positions.”
- Level 3: CA and RA shall have a BI (Background Investigation) using Standard Form 86, “Questionnaire for National Security Positions.”
- Level 4: CAs and RAs shall have an SSBI (Single Scope Background Investigation) using Standard Form 86, “Questionnaire for National Security Positions.”

j) **CA Compromised or Disabled**

If a CA is compromised or unable to function, the bureau shall notify the PMA immediately and implement restoration in accordance with the approved CPS. The PMA shall conduct an audit of the restored CA.

b. **Procedures**

Exceptions and waivers to the PKI policy and standards should require that a written request signed by the bureau CIO be submitted to the PMA. Approval must be received before implementation of a policy or standard variance.

5.5.3 Public Key/Private Key

Public and private keys must be managed properly to ensure their integrity. The integrity of the public key is established through a digital certificate issued by a CA that cryptographically binds the individual's identity to his or her public key. Binding the individual's identity to the public key corresponds to the protection afforded to an individual's private signature key.

A PKI includes an ability to recover from situations in which an individual's private signature key is lost, stolen, compromised, or destroyed; this is done by revoking the digital certificate that contains the private signature key's corresponding public key.

a. **Standards**

1) Protect the private key from disclosure because failing to do so would allow someone to masquerade as that user. Private keys shall be protected using, at a minimum, a strong password, in accordance with Section 5.1.1 of this handbook.

2) Users shall report any suspected loss or compromise of the private keys to the bureau incident response team.

b. **Procedures**

If at all possible, keep private keys stored separately from the workstation or laptop.

5.6 VIRUS PROTECTION

Malicious software presents an increasingly serious security problem for computer systems and networks. Malicious software includes viruses, Trojan horses, and worms. A Trojan horse is a program that appears to perform a useful function, but also includes an unadvertised feature that is usually malicious in nature. Viruses can be hidden in Trojan horses. Viruses and other malicious software can spread quickly through software bulletin boards, shareware, and users' unknowingly copying and sharing these programs in an unauthorized manner. Networks are particularly vulnerable because they allow the very rapid spread of the virus and worms to all systems connected to the network.

a. **Standard**

Bureaus, employees, and contractors shall not disable the antivirus software.

b. **Procedure**

1) Bureaus should inform all employees and contractors of the following information as part of the security awareness briefing:

   a) What is malicious code

   b) How do I report malicious software.

2) Bureaus should establish appropriate file/protocol/content filtering procedures approved by their Chief Counsel.

5.7 PRODUCT ASSURANCE

Computer security assurance provides a basis for confidence that security measures, both technical and operational, work as intended. Varying degrees of assurance are supported through methods such as conformance testing, security evaluation, and trusted development methodologies. Assurance is not, however, a guarantee that the measures will work as intended; it is closely related to reliability and quality.

The Common Criteria program is a joint effort of NSA and NIST, under the National Information Assurance Partnership (NIAP), to evaluate IT product conformance to international standards. The program is a partnership between the public and private sectors. The criteria are implemented not only to help consumers in selecting commercial off-the-shelf IT products that will meet their security requirements but also to help the manufacturers of these products in gaining acceptance in the global marketplace. The program objectives are as follows:

- Meet the needs of government and industry for cost-effective evaluation of IT products
- Encourage the formation of commercial security testing laboratories and the development of a private sector security testing industry
- Ensure that security evaluations of IT products are performed to consistent standards
- Improve the availability of evaluated IT products.

The criteria provide an internationally recognized basis for specifying and testing a wide range of security technology, from components to products and systems. The Common Criteria will permit comparability between the results of independent security evaluations. They do so by providing a common set of requirements for the security functions of IT products and systems and for assurance measures applied to them during a security evaluation. The evaluation process establishes a level of confidence that the security functions of such products and systems and the assurance measures applied to them meet these requirements. The Common Criteria address protection of information from unauthorized disclosure, modification, or loss of use.

The protection profile contains a set of security requirements, either from the Common Criteria or stated explicitly, which should include an evaluation assurance (EA) level. The protection profile permits the implementation-independent expression of security requirements for a set of target evaluations that will comply fully with a set of security objectives. A protection profile is intended to be reusable and to define target-of-evaluation requirements that are known to be useful and effective in meeting the identified objectives, both for functions and assurance. The

protection profile also contains the rationale for security objectives and security requirements. It can be a statement of customers, consumers, and/or a consortium of user needs for the implementation-independent requirements of a product or system.

a. **Standards**

E-ITSPA shall evaluate registered protection profiles for use by Treasury.

b. **Procedures**

Bureaus should create their own protection profiles for security requirements unique to their bureau.

6. INCIDENT RESPONSE PROCEDURES

The Department of the Treasury Incident Response Procedures provide guidance to Treasury bureau, DO, Treasury OIG, and TIGTA staff on responding to and reporting security incidents that affect the Department of the Treasury's ability to conduct its mission.

The incident response procedures apply to all Treasury bureaus, DOs, the Treasury OIG, and TIGTA.

6.1 INCIDENT RESPONSE CAPABILITY OVERVIEW

An incident response capability serves as a mechanism for receiving and/or disseminating incident information and provides a consistent capability to respond to and report on incidents.

The incident response capability within the Department of the Treasury functions in accordance with federal policy and regulation, including OMB Circular A-130, Appendix III, Security of Federal Automated Information Resources; PDD-63, *Critical Infrastructure Protection*; and FISMA. The incident response capability supports the Security Incident and Violation Handling policy in the Treasury IT Security Program Policy.

The incident response capability also provides the following:

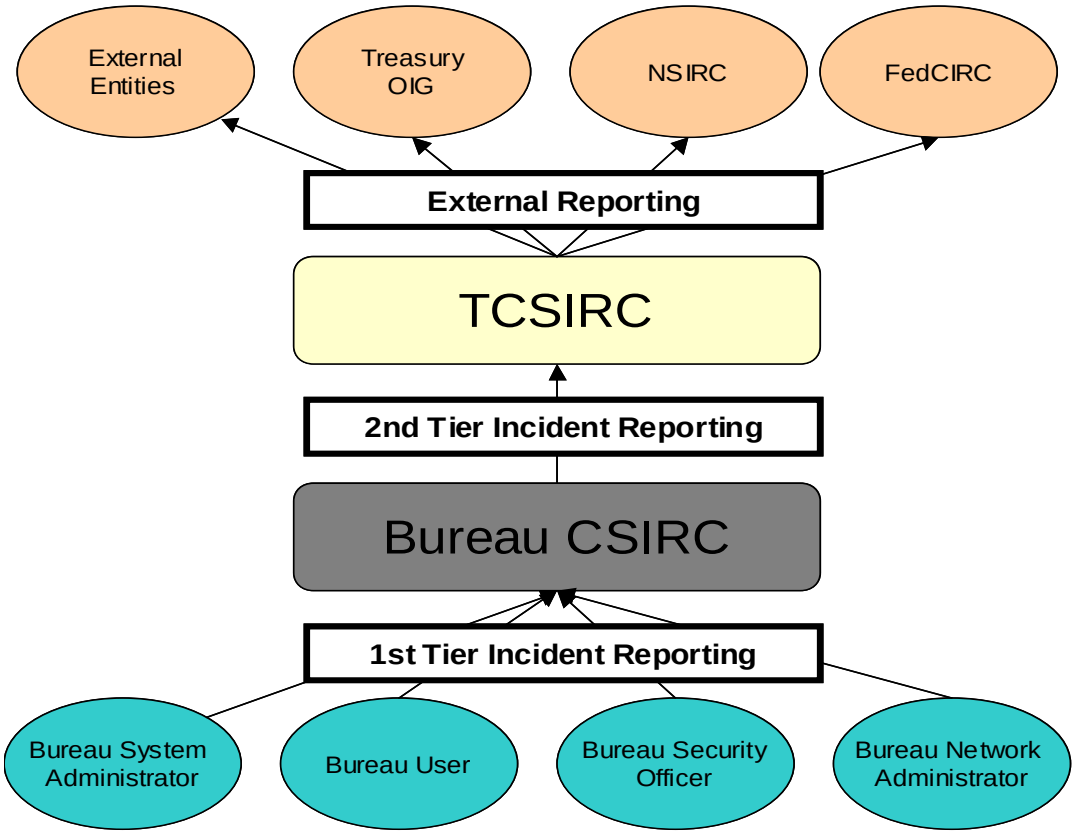
- A framework for identifying, handling, managing, responding to, and reporting incidents in a timely and expeditious fashion
- A mechanism for disseminating generic and specific incident information to the CIOs and bureaus to ensure that actions are being taken to minimize the impact of ongoing or potential incidents
- Governmentwide information sharing of threats, incidents, and trends to support security planning and operations.

6.1.1 Treasury Incident Response Capability Structure

In accordance with the Security Incident and Violation Handling policy in TD P 85-01, the Department of the Treasury bureaus, DOs, Treasury OIG, and TIGTA shall establish and maintain a bureau incident response capability to ensure timely reporting of security incidents to the Department of the Treasury Computer Security Incident Response Center (CSIRC). The bureau-level CSIRC hereafter will be referred to as the "bureau CSIRC." The departmentwide CSIRC hereafter will be referred to as the "TCSIRC."

Figure 6-1 illustrates the TCSIRC's relationships within Treasury and with external entities.

Figure 6-1. TCSIRC Structure



The TCSIRC serves as a 24x7x365 escalation center and as the central point of contact for incidents for the Department of the Treasury. The TCSIRC facilitates incident reporting to the Treasury OIG and to external reporting entities, including the FedCIRC, the National Infrastructure Protection Center (NIPC), the National Security Incident Response Center (NSIRC), and others such as the Information Sharing and Analysis Centers (ISAC).

6.1.2 TCSIRC Functions

The TCSIRC offers security incident handling services, including—

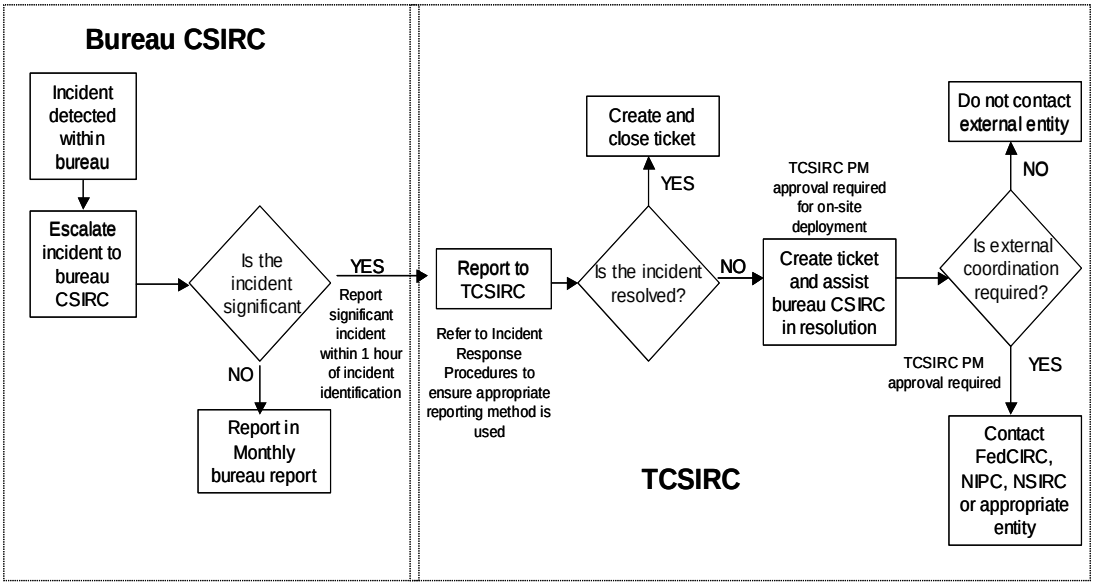
- **Offsite Support.** The TCSIRC serves as the second-tier support for coordination and analysis of security incidents; the bureau CSIRC provides the first-tier support. TCSIRC support is typically conducted via telephone and includes technical advice and mitigation strategies for security incidents as needed.
- **Onsite Support.** On an as-requested basis, the TCSIRC participates in security incident handling efforts onsite at the affected bureau.
- **Advisories and Vulnerability Bulletins.** The TCSIRC is responsible for providing timely dissemination of security-related advisories and countermeasures to the bureau CSIRCs. The advisories and vulnerability bulletins are available to the bureau CSIRCs through the Web portal.

- **Incident Reports.** The TCSIRC is responsible for facilitating incident reporting to external entities, maintaining a database of incidents reported, and compiling both sanitized and unsanitized reports.

6.1.3 Incident Reporting Process Flow

Bureau CSIRCs are required to report significant incidents to the TCSIRC. The TCSIRC shall assist, if necessary, in the incident handling process and facilitate coordination with external entities. Figure 6-2 displays the incident response process for incident reporting from the bureau CSIRCs to the TCSIRC.

Figure 6-2. Incident Reporting Process Flow



6.1.4 Incident Priority Levels

When handling an incident, the TCSIRC incident handler, with assistance from the bureau CSIRC, shall determine the impact of the incident on the bureau's and the Department of the Treasury's computing environment. Incident impact is calculated using one of five priority levels (shown in Table 6-1).

Priority 1 is the highest priority level; Priority 5, the lowest. If multiple incidents occur simultaneously, each incident shall be addressed according to its priority level.

Table 6-1. Incident Priority Levels

Priority Level	Definition
Priority 1	Protect human life and safety. Protection of human life always takes precedence over all other considerations.
Priority 2	Protect classified data as regulated by government statutes and regulations.
Priority 3	Protect sensitive data, including proprietary, financial, law enforcement, scientific, and managerial data. This includes "CIP Assets".

Priority Level	Definition
Priority 4	Prevent system damage (e.g., loss or alteration of system files, damage to hard drives).
Priority 5	Minimize disruption of computing resources. In many cases, it is better to shut down a system or disconnect from a network than to risk damage to data or systems.

6.1.5 Incident Response Definitions

The key terms defined below are used in the Department of the Treasury Incident Response Procedures:

- **Event.** A notable occurrence, not yet assessed, in a computing or telecommunications system or network that may affect that system or network.
- **Incident.** The violation of an explicit or implied security policy in a computing or telecommunications system or network.
- **Vulnerability.** A weakness in a computing or telecommunications system or network, system security procedures, internal controls, or implementation that could be exploited.
- **Minor Incident**. A security-related incident classified as—
  - Misuse of resources
  - Loss or theft of equipment containing nonsensitive information
  - Probe or reconnaissance scan
  - Unsuccessful access or penetration attempt
  - Malicious code detection.
- **Significant Incident.** A security-related incident classified as—
  - Unauthorized alteration or compromise of data
  - Classified incident
  - DoS attack
  - DNS attack
  - Loss or theft of equipment containing sensitive or classified information
  - Successful malicious code infection (not detected by antivirus software)
  - Root compromise
  - Unauthorized access
  - Web site defacement
  - Other (does not fit into a category above).
- **Classified Incident.** Any event that involves a system used to process national security information, a CIP Asset, or any discovery of classified information on any system not certified for that level of classified information (e.g., Secret information on a system not certified to process classified information; Top Secret information on a system certified only for processing Secret information).

See Appendix E for definitions of significant and minor security incident types and Appendix F for additional definitions of security-related terms used in this document.

6.1.6 Roles and Responsibilities

The roles and associated responsibilities for the incident response functionality within the Department of the Treasury are described below.

a. **DASIS/CIO**

The DASIS/CIO has responsibility for—

1) Establishing a Treasury-wide CSIRC
2) Reporting and referring incidents to the Office of the Special Assistant to the Secretary (National Security) when those incidents involve IT systems that process, store, or transmit foreign intelligence information
3) Establishing partnering agreements with federal incident response capabilities
4) Establishing partnering agreements for law enforcement support for security-related incidents with the Treasury OIG and TIGTA
5) Ensuring that all Treasury bureaus, DOs, the Treasury OIG, and TIGTA maintain a separate CSIRC capability that serves as the first tier of incident response and reporting.

b. **Special Assistant to the Secretary (National Security)**

The Special Assistant to the Secretary (National Security) has responsibility for establishing incident response and reporting procedures for IT systems that process, store, or transmit foreign intelligence information.

c. **TCSIRC Project Manager (PM)**

The identified TCSIRC PM, or backup PM, maintains responsibility for—

1) Serving as primary interface between the TCSIRC and 24x7x365 operations and Department of the Treasury management and bureaus
2) Establishing and implementing tools and processes supporting the bureau CSIRCs' policies and procedures to ensure timely reporting of security incidents
3) Developing and maintaining these procedures and the supporting policy in TD P 85-01
4) Approving incident reports before distributing them Treasury-wide or releasing them to external entities
5) Approving onsite deployment of a TCSIRC incident handling team to a bureau location.

d. **TCSIRC**

The TCSIRC has responsibility for—

1) Serving as the primary clearinghouse and collection point for incident information involving Treasury systems or networks for the Department of the Treasury

2) Assisting the bureaus with technical issues and investigations involving security incidents

3) Coordinating with external incident response organizations as directed in reporting procedures

4) Offering services, such as early warnings and malicious code alerts, to the bureaus

5) Coordinating with bureau CSIRCs on incident reporting, incident handling, and incident prevention activities

6) Serving as the second tier of incident response and reporting, for example, providing advice and/or onsite assistance on security incidents if requested by an authorized representative of the bureau

7) Reporting incident trends to the TCSIRC PM based on the significance of the trend

8) Keeping the TCSIRC PM apprised of reported significant security incidents and interactions with external reporting entities

9) Reporting and coordinating with the Treasury OIG on validated criminal security incidents.

e. **Heads of Bureaus, the Treasury OIG, and TIGTA**

The heads of bureaus, the Treasury OIG, and TIGTA have responsibility for the following for their respective bureaus and offices:

1) Establishing a bureau CSIRC to serve as the first tier of incident response and the investigative and reporting body

2) Developing and maintaining the bureau CSIRC policy and procedures

3) Enforcing processes and procedures developed by the TCSIRC.

f. **Bureau CSIRC**

The bureau CSIRC has responsibility for—

1) Serving as the first tier of incident response at the bureau level and investigating, coordinating, and reporting incidents to the TCSIRC

2) Reporting significant incidents to the TCSIRC within 1 hour of incident identification, with a follow-up report every 4 hours thereafter until the incident is resolved

3) Providing monthly summary reports of minor incidents to the TCSIRC by the fifth calendar day of each month for incidents that occurred the previous month

4) Writing lessons learned and follow-up reports on bureau incidents

5) Establishing and implementing tools and processes supporting the bureau CSIRC's policies and procedures to ensure timely reporting of security incidents.

g. **System Administrators, Network Administrators, Security Officers, and Users**

System administrators, network administrators, security officers, and users of computing or telecommunications systems or network resources provided by the Department of the Treasury, including any government personnel or contractors, shall report incidents immediately upon recognition or suspicion of an event. Reporting shall comply with Department security incident policy and any bureau-specific policy requirements.

6.2 INCIDENT REPORTING REQUIREMENTS

This section outlines the incident reporting and associated requirements for the TCSIRC and the bureau CSIRCs.

6.2.1 TCSIRC Reporting Requirements

The TCSIRC serves as the second-tier reporting function for the Department of the Treasury, and as the interface to external organizations.

6.2.1.1 Individual Incident Reports

The bureau CSIRC shall notify the TCSIRC upon identification of a significant incident and report minor incidents to the TCSIRC in a monthly summary report. The TCSIRC shall notify the TCSIRC PM when a significant incident has been reported to the TCSIRC, in accordance with the TCSIRC standard operating procedures.

Communications and data storage related to an incident shall be conducted in accordance with the security incident's classification or sensitivity.

If the incident involves an IT system that processes, stores, or transmits foreign intelligence information, the incident shall be reported to the Special Assistant to the Secretary (National Security).

Unsanitized reports are compiled on an as-requested basis and shall be classified in accordance with the Office of Information Systems Security *Security Control Guide for the Department of the Treasury's Sensitive Critical Information Assets Associated with Project Matrix* (dated February 1, 2002) and the associated classification guide (dated February 20, 2002). Unsanitized reports shall be marked and handled appropriately.

The process for incident resolution is documented in a database maintained by the TCSIRC. This database serves as a repository for the summary reports of individual incidents reported to TCSIRC. The database is available to the bureau CSIRCs through a secure Web portal.

The TCSIRC PM shall be notified upon closure of the significant incident in accordance with the TCSIRC standard operating procedures.

6.2.1.2 Weekly Activity Summary Report

The weekly activity summary report, summarizing the total number of significant incidents reported during the preceding week, is available to the TCSIRC PM through a secure Web portal.

6.2.1.3 Monthly Summary Report

The TCSIRC is responsible for aggregating the monthly bureau summary reports received from the bureau CSIRCs into a Department-level sanitized monthly summary report. Bureaus' monthly summary reports are due the fifth calendar day of each month for minor incidents that occurred the previous month. To process the online monthly report form, choose Monthly Submit from the EVENTS page after logging on to the Web portal. The sanitized monthly summary report is available to the TCSIRC PM through a secure Web portal.

The TCSIRC sanitized and unsanitized monthly summary reports are due to the PM by the 10th calendar day of the month for incidents that occurred during the previous month. Items that shall be included in the monthly report are as follows:

a. **Top 5 IP addresses.** Report the five originating IP addresses that generated the most activity reported across all minor incidents.

b. **Misuse of Resources.** Report the total number of occurrences of an authorized user's mishandling a resource (e.g., computing or telecommunications system or network).

c. **Loss or Theft of Equipment With Unclassified Information.** Report the total number of equipment items (e.g., workstations, laptops, or any other telecommunications or computer equipment that could contain Treasury data) containing nonsensitive data or information that are lost, missing, or stolen.

d. **Probes and Reconnaissance Scans.** Report the total number of occurrences of suspicious probing or scanning of networks for critical services or security weaknesses.

e. **Unsuccessful Access and Penetration Attempts.** Report the total number of suspicious unsuccessful access or penetration attempts (e.g., Nimda or Code Red scans).

f. **Malicious Code Detection.** Report the total number of times malicious code was detected and cleaned by antivirus software.

g. **Other.** Report the total number of occurrences of minor incidents that do not fall into any of the aforementioned categories and are not defined as a significant incident.

6.2.1.4 Reporting to Internal and External Entities

The TCSIRC is the central point of contact for coordinating all incident response and reporting within the Department of the Treasury and between Treasury bureaus and outside entities (e.g., FedCIRC, NSIRC, NIPC, and ISACs). Coordination with law enforcement and/or NIPC shall be conducted primarily by, or in conjunction with, the Treasury OIG.

6.2.1.5 FedCIRC

The TCSIRC automatically reports all significant incidents to FedCIRC. Information requests from FedCIRC shall be filtered through the TCSIRC PM before information is released.

6.2.1.6 Treasury OIG and Law Enforcement

An MOU has been established between the Department of the Treasury and the OIG for triage and investigation support. The TCSIRC coordinates escalation to the Treasury OIG for all validated criminal security incidents. Coordination with law enforcement and/or NIPC shall be conducted primarily by, or in conjunction with, the Treasury OIG.

6.2.1.7 NSIRC

The TCSIRC automatically reports foreign IP addresses identified in both significant and minor incidents to NSIRC. Classified incidents shall also be reported to NSIRC.

6.2.1.8 Other Internal and External Entities

The TCSIRC PM's approval is required before Treasury security incident-related information is reported to other internal or external entities. This includes coordinating communication with organizations such as the Computer Emergency Response Team (CERT) Coordination Center, and other security incident response organizations.

6.2.2 Bureau CSIRC Reporting Requirements

The bureau CSIRCs serve as the first-tier incident reporting function for the system administrators, network administrators, security officers, and users within the bureau. The bureau CSIRC is responsible for reporting an incident to the TCSIRC.

6.2.2.1 Individual Incident Reporting

The bureau CSIRCs have the following responsibilities in individual incident reporting:

- **Minor Incident.** The bureaus shall document minor incidents in a summary report and provide the report to the TCSIRC on a monthly basis. (See Section 6.2.1.3 for monthly incident reporting procedures.)
- **Significant Incident.** Upon identification of a significant incident, the bureau CSIRC shall provide a preliminary report to the TCSIRC within 1 hour. Within 4 hours of the initial report, the bureau CSIRC shall provide a more detailed report. The bureau CSIRC shall update the TCSIRC every 4 hours until incident resolution and shall update the TCSIRC as new information is discovered about the incident. Because significant incidents are reported on a per-incident basis, they should not be included in the monthly summary report. (See Section6.1.5 for definition of "significant incident.")

When reporting a significant incident, the bureau CSIRC shall provide the information outlined in the Incident Report Form in Appendix C.

6.2.2.2 Monthly Incident Reporting

Bureau CSIRCs shall generate monthly reports for the TCSIRC. Bureaus' monthly reports are due the fifth calendar day of each month for minor incidents that occurred during the previous month. Because significant incidents are reported on a per-incident basis, they should not be included in the monthly summary report. Bureau monthly reports summarize the past month's minor incidents and may include changes to point-of-contact information, improvement suggestions, and other incident response issues of concern to the bureau.

Note: If classified system incidents are included in the monthly report, the report shall be sanitized to avoid unauthorized disclosure. Reports containing classified information shall be reported through appropriate secure communications (e.g., STU-III, secure fax).

Bureau CSIRCs can use the online Monthly Summary Report Form. If the online form is not used, the bureau's monthly report should contain the items listed below. A sample format for the monthly report is provided in Appendix D.

a. **Summary of Minor Incidents**

   1) **Top 5 IP Addresses.** Report the five originating IP addresses that generated the most activity across all minor incidents

   2) **Misuse of Resources.** Report the total number of occurrences

   3) **Loss or Theft of Equipment With Unclassified Information.** Report the total number of occurrences

   4) **Probes and Reconnaissance Scans.** Report the total number of occurrences

   5) **Unsuccessful Access and Penetration Attempts.** Report the total number of occurrences

   6) **Malicious Code Detection.** Report the total number of times malicious code was detected and cleaned by the antivirus software.

b. Any additional information, such as feedback on the TCSIRC's performance, other incidents, or changes in bureau point-of-contact information.

6.2.2.3 Reporting to FedCIRC, NIPC, Law Enforcement, NSIRC, Treasury OIG, and External Entities

Incident reporting to FedCIRC, the Treasury OIG and law enforcement, NIPC, NSIRC, and other external entities shall be coordinated through the TCSIRC.

6.2.2.4 Bureau CSIRC Incident Reporting Guidelines

This section outlines incident reporting guidelines on significant incidents to ensure the confidentiality of the information reported. Minor incidents should be reported monthly. A sample format for the monthly report is provided in Appendix D.

6.2.2.5 Bureau CSIRC

The bureau CSIRC shall report information on significant incidents on the Incident Report Form presented in Appendix C, and shall follow the guidelines in Sections 3.3.1.1 through 3.3.1.3, as applicable to the bureau's systems.

6.2.2.6 Unclassified System

The bureau CSIRCs can report incidents occurring on unclassified systems to the TCSIRC through the following methods:

- E-mail
- Fax
- Telephone
- Online incident report.

See Appendix A for TCSIRC contact information.

6.2.2.7 Critical Information Assets Associated with Project Matrix (CIP Asset)

Bureau CSIRCs shall take additional precautions when reporting incidents involving a critical information asset associated with Project Matrix, (i.e., a CIP Asset). Incidents shall be classified in accordance with the Office of Information Systems Security *Security Control Guide for the Department of the Treasury's Sensitive Critical Information Assets Associated with Project Matrix* (dated February 1, 2002) and the associated classification guide (dated February 20, 2002). CIP Asset incidents shall be reported using secure communications, such as—

- STU-III
- Secure fax.

6.2.2.8 Classified Incidents (or Systems Supporting Foreign Intelligence Information)

The bureau CSIRC shall report classified incidents to the TCSIRC using secure communications, such as—

- STU-III
- Secure fax.

After the bureau CSIRC has reported the classified incident to the TCSIRC, the TCSIRC shall report all classified incidents to the NSIRC. If the classified incident involves systems with foreign intelligence information, the TCSIRC shall report the incident to the Special Assistant to the Secretary (National Security).

6.2.2.9 TCSIRC

When a significant incident is reported to the TCSIRC, the TCSIRC PM shall be notified. The TCSIRC maintains a database of all significant incidents. The database is accessible to the bureau CSIRC points of contact designated by the reporting bureau and to the TCSIRC PM.

Open incidents are accessible only to the reporting bureau and the TCSIRC PM. After sanitization, closed incidents are available to the other bureaus.

Incidents shall be handled in accordance with their sensitivity and classification. The TCSIRC incident handler shall follow the appropriate TCSIRC SOP. For classified reports, or incidents involving a CIP Asset, a secure fax or STU-III shall be used. The TCSIRC security plan shall be followed to ensure that classified information is stored appropriately.

Upon incident closure, the TCSIRC shall inform the PM of resolution.

6.3 INCIDENT HANDLING

Typically, incident handling consists of six stages:

- **Preparation.** Establish an approach to incident handling, including developing policy and procedures, defining an incident, and identifying components required in a response effort.
- **Identification.** Analyze detection components (e.g., IDSs, firewalls, audit logs) to identify signs of an incident, notify appropriate officials of an incident, and begin handling the evidence to ensure a verifiable chain of custody.
- **Containment.** Ensure that the incident does not grow worse.
- **Eradication.** Determine the cause and remove the cause.
- **Recovery.** Restore to the original state and validate the clean system.
- **Follow-Up.** Develop follow-up reports, identify lessons learned, and update procedures as necessary.

6.3.1 Bureau CSIRC Support

The bureau CSIRC serves as the first tier in incident handling. It assists the reporting party (e.g., system administrator, network administrator, security officer, or user). The bureau CSIRC also reports significant incidents to the TCSIRC and can request assistance on the incident from the TCSIRC for offsite or onsite assistance.

The bureau CSIRC plays a role in all six incident handling stages, described below.

6.3.1.1 Preparation

The bureau CSIRC shall develop and maintain a foundation to support the incident response capability. The preparation activities consist of, but are not limited to, developing the bureau capability policy and procedures, identifying supporting roles and responsibilities, and establishing and implementing the tools and processes supporting the bureau CSIRC's policy and procedures to ensure timely reporting of security incidents. The bureau CSIRC procedures should include procedures to ensure appropriate documentation and chain of custody.

6.3.1.2 Identification

In incident identification, the bureau CSIRC shall first coordinate with network services to determine whether the suspicious event may have been caused by a misconfiguration or some other action. Once it has been confirmed that a security incident has occurred, the team shall determine what type of security incident occurred and how many systems were affected. At this point, the bureau CSIRC may call the TCSIRC for assistance in the containment, eradication, and recovery stages.

6.3.1.3 Containment

Once the incident has been identified, the bureau CSIRC shall assist the reporting party in containment activities. At this point, the risk of continuing to operate the affected system is determined. Containment activities may include—

- Performing a full backup onto unused media and safely storing it for law enforcement officials
- If possible, making a second full backup for comparison purposes
- Keeping all incident handlers informed and advising the system owners of progress
- Gathering router and system logs for review, as well as logs from interconnected systems
- Changing passwords on the compromised systems and on all systems that interact with the compromised systems

6.3.1.4 Eradication

The bureau CSIRC shall help the reporting party determine the symptoms and the cause of the incident. If the cause cannot be determined, a best guess based on the evidence at hand should be made and included with the initial report. The condition that was exploited to cause the incident shall be corrected and the most recent clean backup located.

6.3.1.5 Recovery

Once the system is again performing normally, it must be tested and validated before it is brought back online on a production network. Every effort shall be made not to restore back doors or malicious code. For example, if a root kit installation is suspected, the system should be reformatted and the operating system should be rebuilt, including all patches and fixes, before redeployment. However, these changes could effectively destroy evidence. Therefore, if the incident is being investigated by law enforcement, it is necessary to obtain the concurrence of the investigator before making changes of this nature. Applications and data should then be reloaded on the fresh operating system.

6.3.1.6 Follow-Up

A follow-up report shall be written as soon as possible to ensure a full and accurate account of all details. Policies and procedures shall be modified as required.

6.3.1.7 Escalating Priority of Incidents

An incident's priority may change as more information becomes available. If an incident becomes more critical, the bureau CSIRC incident handler in charge shall update the incident report and inform the rest of the incident handling team and the TCSIRC so that the appropriate attention can be given to the incident.

6.3.2 TCSIRC Support

At a bureau's request, the TCSIRC shall assist the bureau CSIRC through the incident handling process. However, if onsite support is needed, the TCSIRC PM's approval is required before TCSIRC incident handlers are dispatched to the site.

6.3.2.1 Receiving Incident Calls

In incident identification, the bureau CSIRC shall first coordinate with network services to determine whether the suspicious event may have been caused by a misconfiguration or some other action. Once it has been confirmed that a security incident has occurred, the team shall determine what type of security incident occurred and how many systems were affected. At this point, the bureau CSIRC may call the TCSIRC for assistance in the containment, eradication, and recovery stages.

Once the TCSIRC incident handler receives the initial call from the bureau CSIRC, the incident handler may need to help determine whether an event is a security incident. The bureau CSIRC should provide the TCSIRC incident handler with as much information as possible. (See Appendix C, Treasury Computer Incident Report Form.)

The incident handler shall first determine whether the event resulted from some inadvertent activity (e.g., a simple mistake, such as misconfiguration, or recent network architecture changes). Suspicious events shall be given the same attention as confirmed security incidents until they are proved *not* to be security incidents. False positives should be handled effectively to encourage continued security incident reporting.

If multiple incidents are received, response shall be prioritized based on the incident priority levels presented in Section 6.1.4.

6.3.2.2 Gathering Information

Once it is determined that a security incident has occurred, the TCSIRC incident handler shall gather as much information as possible. If there is any chance that the incident may involve law enforcement, the incident handler shall advise the bureau capability to carefully maintain a verifiable chain of custody by tracking physical access to the systems and devices. Coordination with law enforcement is conducted through the Treasury OIG.

6.3.2.3 Recording Incidents

The TCSIRC incident handler shall record significant incidents according to the information gathered. Possible response scenarios are as follows:

- **Incident Is Resolved Before Reporting.** If the incident has already been resolved, and no further action is required, the incident handling process is closed out.
- **Incident Is Resolved, but Further Action Is Required.** If the incident has been resolved, but further action is required, such as contacting the Treasury OIG or an outside organization (e.g., FedCIRC), the TCSIRC initiates that process as outlined in the Treasury Incident Response Procedures and the TCSIRC standard operating procedures.
- **Incident Is Ongoing.** The bureau CSIRC notifies the TCSIRC within 1 hour of incident identification, with an update every 4 hours after initial notification until incident resolution. If the incident is ongoing and the bureau CSIRC has not requested assistance from the TCSIRC, the TCSIRC incident handler contacts the bureau capability to discuss the status of the incident within 24 hours of the incident report. Once the incident has been resolved, it is closed out.
- **Request for Onsite Assistance With an Ongoing Incident.** When a bureau CSIRC requests onsite assistance with an ongoing incident, the incident handler notifies the TCSIRC PM. If assistance is approved, the TCSIRC PM coordinates TCSIRC onsite assistance to the bureau. When the incident is resolved, the TCSIRC incident handler on duty should update and close the incident.

6.3.2.4 Closing Out Incidents

Once the incident has been resolved, the bureau CSIRC and/or the TCSIRC incident handler shall report the incident as closed. If any additional information (e.g., firewall logs, intrusion detection logs, chain of custody logs, or other reports gathered by the bureau capability during the course of its investigation) becomes available after the incident is reported closed, that information should be forwarded to the TCSIRC to be included in the TCSIRC's incident report.

6.3.2.5 Following Up On Incidents

The bureau CSIRC is responsible for writing the lessons learned report. The bureau CSIRC may use the incident report stored in the secure Web portal that is maintained by the TCSIRC and may coordinate with the TCSIRC to ensure that the information in the lessons learned report is accurate.

A bureau may also request assistance from the TCSIRC in securing its system as a follow-up to an incident.

6.3.2.6 Escalating Priority of Incidents

An incident's priority may change as more information becomes available. When that occurs, the TCSIRC incident handler shall update the incident report and inform the rest of the incident handling team, the bureau CSIRC, and the TCSIRC PM.

6.3.3 Onsite Incident Handling

At the request of the bureau CSIRC, the TCSIRC shall forward requests for onsite assistance from the bureau capability to the TCSIRC PM. Upon approval of the PM, the PM shall

coordinate onsite visits, including forwarding visitor requests to the bureaus. The PM and the TCSIRC shall assist the bureau CSIRC in incident handling. Onsite support responsibilities for the TCSIRC incident handler include, but are not limited to, the following:

- Documenting the incident
- Acting as a liaison between the bureau and the TCSIRC
- Ensuring that Department incident handling guidelines and best practices are followed
- Containing damage
- Creating backups, if possible, of the affected systems
- Resolving the problem
- Resuming business.

To prevent duplicative efforts, the onsite TCSIRC incident handler shall ensure that only one individual is in charge and that each team member reports to that person. Typically, the bureau CSIRC is in charge of incident handling within its bureau with the assistance of the TCSIRC onsite team. The TCSIRC incident handler team is responsible for providing reports to the TCSIRC as each phase is completed, once a day, or when there are significant changes in the incident's status. The TCSIRC shall provide updates to the TCSIRC PM.

6.4 INCIDENT PREVENTION REQUIREMENTS

Incident prevention activities consist of alerts and advisories that originate from the TCSIRC.

6.4.1 Bureau CSIRC Responsibilities

The bureau CSIRC is responsible for distributing advisories and vulnerability bulletins received from the TCSIRC, either through e-mail or through telephone or pager call to the appropriate individuals within the bureau (e.g., network operations centers, system administrators, ISSOs).

6.4.2 TCSIRC Responsibilities

The TCSIRC is responsible for providing timely dissemination of advisories and vulnerability bulletins to the designated points of contact within each bureau CSIRC. Advisories and vulnerability bulletins shall be made available to the bureau CSIRCs through the Web portal.

The TCSIRC also serves as the first point of contact for any bureau researching an anomaly. The TCSIRC is the primary interface in the Department of the Treasury for third-party-organization reporting of security incidents, vulnerabilities, and countermeasures released. The TCSIRC shall coordinate with third parties to answer any questions a bureau might have.

7. ACRONYMS

AES	Advanced Encryption Standard
ANSI	American National Standards Institute
ASM	Assistant Secretary for Management
ASSET	Automated Security Self-Evaluation Tool
BI	Background Investigation
C&A	Certification and Accreditation
CA	Certification Authority
CCB	Configuration Control Board
CERT	Computer Emergency Response Team
CFO	Chief Financial Officer
CFR	Code of Federal Regulations
CGI	Common Gateway Interface
CIAO	Critical Infrastructure Assurance Officer
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CIPO	Critical Infrastructure Protection Officer
CIRB	Capital Investment Review Board
CNSS	Committee for National Security Systems
CPS	Certification Practice Statement
CRB	Change Review Board
CRT	Cathode Ray Tube
CSIRC	Computer Security Incident Response Capability
CSRC	Computer Security Resource Center
DAA	Designated Accrediting Authority
DAC	Discretionary Access Control
DASIS	Deputy Assistant Secretary for Information Systems
DES	Data Encryption Standard
DMZ	Demilitarized Zone
DO	Departmental Office
DoS	Denial of Service
DRAM	Dynamic Random Access Memory
EA	Evaluation Assurance
EAPROM	Electronically Alterable Programmable Read Only Memory
EEPROM	Electronically Erasable PROM
EFT	Electronic Funds Transfer
E-ITPO	Enterprise Information Technology Planning and Operations
E-ITSPA	Enterprise Information Technology Security Planning and Assurance
E-mail	Electronic Mail
E.O.	Executive Order
EPF	Employee Personnel File
EPROM	Erasable Programmable Read Only Memory

FAM	Foreign Affairs Manual
Fax	Facsimile
FBI	Federal Bureau of Investigation
FedCIRC	Federal Computer Incident Response Capability
FEMA	Federal Emergency Management Agency
FEPROM	Flash EPROM
FIPS	Federal Information Processing Standards
FISCAM	Federal Information System Controls Audit Manual
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act
FTE	Full-Time Equivalent
FTP	File Transfer Protocol
FY	Fiscal Year
GAO	General Accounting Office
GRS	General Records Schedule
GSA	General Services Administration
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HVAC	Heating, Ventilation, and Air-Conditioning
I&A	Identification and Authentication
IA	Information Assurance
IATO	Interim Authority to Operate
ICMP	Internet Control Message Protocol
ID	Identification
IDS	Intrusion Detection Systems
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IG	Inspector General
INFOSEC	Information Systems Security
IP	Internet Protocol
IR	Infrared
ISAC	Information Sharing and Analysis Center
ISO	International Organization for Standardization
ISSM	Information Systems Security Manager
ISSO	Information Systems Security Officer
IT	Information Technology
ITL	Information Technology Laboratory
ITMRA	Information Technology Management Reform Act
kbps	Kilobits Per Second
KMI	Key Management Infrastructure

LAN	Local Area Network
LOU	Limited Official Use
MBI	Minimum Background Investigation
MGCP	Multimedia Gateway Control Protocol
MOU	Memorandum of Understanding
NARA	National Archives and Records Administration
NCSC	National Computer Security Center
NFS	Network File Systems
NIACAP	National Information Assurance Certification and Accreditation Process
NIAP	National Information Assurance Partnership
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
NOVRAM	Nonvolatile Random Access Memory
NSA	National Security Agency
NSF	Nonstandard Facilities
NSIRC	National Security Incident Response Center
NSTISS	National Security Telecommunications and Information Systems Security
NSTISSC	National Security Telecommunications and Information Systems Security Committee (renamed CNSS)
NSTISSD	National Security Telecommunications and Information Systems Security Directive
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
OIG	Office of the Inspector General
OMB	Office of Management and Budget
OPF	Official Personnel File
OSI	Open Systems Interconnect
OTAR	Over-the-Air Rekeying
PBX	Private Branch Exchange
PC	Personal Computer
PDD	Presidential Decision Directive
PED	Portable Electronic Device
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
PM	Project Manager
PMA	Policy Management Authority
POA&M	Plan of Actions and Milestones
PROM	Programmable Read Only Memory

QA	Quality Assurance
RA	Registration Authority
RAM	Random Access Memory
RF	Radio Frequency
RIP	Routing Information Protocol
ROM	Read Only Memory
RPC	Remote Procedure Call
SF	Standard Form
SIP	Session Initiation Protocol
SOW	Statement of Work
SP	Special Publication
SRAM	Static Random Access Memory
SSAA	System Security Authorization Agreement
SSBI	Single Scope Background Investigation
SSI	Server Side Includes
SSP	System Security Plan
ST&E	Security Test and Evaluation
TCI	Treasury Critical Infrastructure
TCIPP	Treasury Critical Infrastructure Protection Plan
TCP	Transmission Control Protocol
TCSIRC	Treasury Computer Security Incident Response Capability
TD	Treasury Directive
TD P	Treasury Directive Publication
TIGTA	Treasury Inspector General for Tax Administration
TIPP	Treasury Infrastructure Protection Panel
TO	Treasury Order
UDP	User Datagram Protocol
UPS	Uninterruptible Power Supply
URL	Uniform Resource Locator
U.S.C.	United States Code
VoIP	Voice over IP
VPN	Virtual Private Network
WAN	Wide Area Network
WLAN	Wireless Local Area Network
WORM	Write-Once, Read-Many
WWW	World Wide Web

8. DEFINITIONS

Note: Additional IT Security terms can be found in National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 4009.

A

Acceptable Level of Risk

A judicious and carefully considered assessment by the appropriate accrediting authority that the value of the information technology (IT) unambiguously outweighs the likelihood of potential damage to the security interests of the United States in the event information from the system is compromised, damaged, or destroyed. The severity of the potential damage must be taken into account. The assessment should take into account not only the value of IT assets, threats and vulnerabilities, and countermeasures but also their efficacy in compensating for vulnerabilities, and operational requirements.

Access

Opportunity to make use of an information system resource.

Access Control

The process of limiting access to information or to resources of an IT system to only authorized users, programs, processes, or other systems.

Access Control Measures

Hardware and software features, physical controls, operating procedures, management procedures, and various combinations of these designed to detect or prevent unauthorized access to an IT system and to enforce access control.

Accreditation

The official management authorization to operate an IT system: a) in a particular security mode; b) with a prescribed set of administrative, environmental, and technical security safeguards; c) against a defined threat and with stated vulnerabilities and countermeasures; d) in a given operational environment; e) under a stated operational concept; f) with stated interconnections to other IT systems; and g) at an acceptable level of risk for which the accrediting authority has formally assumed responsibility. The accrediting authority formally accepts security responsibility for the operation of an IT system and officially declares that a specified IT system will adequately protect classified or sensitive information against compromise, destruction, or unauthorized alteration through the continuous employment of safeguards, including administrative, procedural, physical, personnel, communications security, emissions security, and computer-based (e.g., hardware, firmware, software) controls. The accreditation statement

affixes security responsibility with the accrediting authority and shows that due care has been taken for security.

Active-X

A technology for implementing object sharing. Active-X controls, which can be developed using a number of programming languages, are a major component of Active-X.

Administrative Security

The management procedures and constraints, operational procedures, accountability procedures, and supplemental controls established to provide an acceptable level of protection for classified information.

Advanced Encryption Standard (AES)

Specifies a Federal Information Processing Standards (FIPS)-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. The AES standard specifies the Rijndael algorithm ([3] and [4]), a symmetric block cipher that can process data blocks of 128 bits, using cipher keys with lengths of 128, 192, and 256 bits. See FIPS PUB 197.

Applet

Java code associated with Hypertext Markup Language (HTML) documents.

Application

The use of information resources (information and IT) to satisfy a specific set of user requirements.

Architecture

The configuration of any equipment or interconnected system or subsystems of equipment that is used in automated acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. Also includes computers, ancillary equipment and services, such as support services and related resources.

Asset

A major application, general support system, high-impact program, physical plant, mission-critical system, or logically related group of systems.

Associated Data Communications

Communications that play many roles for an IT system and for connections among them. The simplest is that of not only connecting geographically nearby users and geographically remote users to a stand-alone IT system, but also interconnecting various components (e.g., multiple host computers) of the central IT equipment. Such associated data communications will be considered in the accreditation of the IT systems using the requirements specified in this volume.

Associated data communications also facilitate the interconnection of multiple IT systems as part of a separately accredited network. In effect, such a separately accredited network, including local area networks (LAN), provides specialized common-carrier data communications to a limited subscriber community. It may be of limited geographic extent (a LAN), of metropolitan area size (tens of kilometers), or wide area (e.g., hundreds of kilometers, national, or worldwide). Separately accredited networks must provide for network security in the form of access safeguards and controls.

Unless they have already been accredited as part of a national telecommunications network, associated data communications, which handle classified data in unencrypted form, must be included in the accreditation of the IT to which they are attached. In this context, associated data communications include items such as protected wire/fiber optic distribution systems, concentrators, multiplexers, and network access devices.

Assurance Testing

A process used to determine that a system's security features are implemented as designed and that they are adequate for the proposed environment. This process may include hands-on functional testing, penetration testing, and/or verification.

Audit

An independent review and examination of system records and activities to test for adequacy of system controls, to ensure compliance with established policy and operational procedures, and to recommend any indicated changes in controls, policy, or procedures.

Audit Trail

A chronological record of system activities to ensure the reconstruction and examination of the sequence of events and/or changes in an event. Audit trail may apply to information in an information system, to message routing in a communications system, or to the transfer of communications security (COMSEC) material.

Authentication

A security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.

Authorization

Access privileges granted to a user, program, or process.

Authorized Person

A person who meets certain access requirements and/or has adequate authorization for sensitive information.

Authorize Processing

See *Accreditation*.

Availability

The timely, reliable access to data and information services for authorized users. This includes the restoration of services after an interruption.

Availability Protection

Protection that requires backup of system and information, contingency plans, disaster recovery plans, and redundancy. Examples of systems and information requiring availability protection are time-share systems, mission-critical applications, time and attendance, financial, procurement, or life-critical.

Awareness, Training, and Education

Awareness, training, and education includes the following: a) Awareness programs set the stage for training by changing organizational attitudes toward realization of the importance of security and the adverse consequences of its failure; b) the purpose of training is to teach people the skills that will enable them to perform their jobs more effectively; and c) education, which is more in depth than training, is targeted at security professionals and those individuals whose jobs require expertise in IT security.

B

Banner

Display on an information system that sets parameters for system or data use.

Bastion Host

A computer on a network specially fortified against network attacks. A bastion host provides a choke point for all communication between a network and the Internet or an extranet.

Boundary of an IT

For purposes of identifying the mode of operation of an IT system to be accredited, the IT system has a conceptual boundary that extends to all intended system users, both directly and indirectly connected, who receive output from the system without a reliable human review by an appropriately cleared authority. The location of such a review is commonly referred to as an "air gap." The perimeter of an IT that encompasses all IT components to be accredited excludes separately accredited networks to which the IT is connected.

Boundary of a Network

For purposes of identifying the mode of a network to be separately accredited (including a LAN), a network boundary extends to (but does not include) the IT systems or other separately accredited networks that attach thereto.

Browsing

Act of searching through information systems storage to locate or acquire information, without necessarily knowing the existence or format of information being sought.

Business Case

A tool that supports planning and decisionmaking. It is used to answer the question, "What are the likely financial and other business consequences if this action or decision is made?" It is a structured request for IT investment projects and a tool that the Government uses to evaluate a) how the IT solution meets the stated business need; b) risks and associated benefits (costs and operational) of the project; and c) how the IT solution meets the organization's business goals.

Business Continuity Planning

The process of developing advance arrangements and procedures, which will enable an organization to respond to an event in such a manner that the essential government functions continue without interruption or essential change.

Business Impact Analysis

The process of determining the impact on an organization should a potential loss identified by the risk analysis actually occur. The business impact analysis shall quantify, where possible, the loss resulting from a business interruption (number of days) and a financial standpoint.

C

Certificate Policy

A document that sets forth the rules established by the policy-issuing entity governing the issuance, maintenance, use, reliance upon, and revocation of digital certificates.

Certification

The comprehensive evaluation of the technical and nontechnical security features of an IT system and other safeguards, made as part of and in support of the accreditation process, that establishes the extent to which a particular design and implementation meet a specified set of security requirements.

Certification Authority (CA)

An entity authorized to sign and issue digital certificates.

Certification Practice Statement (CPS)

A detailed description of the business and operational practices of a CA. A CPS is more detailed than a certificate policy.

Certifier

An individual responsible for making a technical judgment of the system's compliance with stated requirements, identifying and assessing the risks associated with operating the system, coordinating the certification activities, and consolidating the final certification and accreditation packages.

Change Review Board (CRB)

A committee, that acts as a forum, which reviews the proposed non-functional changes and/or improvements to the IT system. The committee provides feedback to the users. Issues that cannot be resolved will be forwarded to the Configuration Control Board (CCB). The membership of the CRB should include the Designated Accrediting Authority (DAA), the Information Systems Security Officer (ISSO), and the system owner. System administrators, network administrators, or database administrators may be called upon to participate in issues brought before the board.

Classified Information

National security information that has been classified pursuant to Executive Order (E.O.) 12958.

Clearing

Removal of data from an information system, its storage devices, and other peripheral devices with storage capacity, in such a way that the data may not be reconstructed using common system capability (i.e., keyboard strokes); however, the data may be reconstructed using laboratory methods. Cleared media may be reused at the same classification level or at a higher level. Overwriting is one method of clearing. Note: Volatile memory can be cleared by removing power to the unit for a minimum of 1 minute.

Common Criteria

International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 15408, Common Criteria for IT Security Evaluation. This is a standard for evaluating IT products and systems, such as operating systems, computer networks, distributed systems, and applications. It states the requirements for security functions and for assurance measures.

Common Gateway Interface

A standard for allowing World Wide Web users to interact with applications running on a remote server.

Communications Security

Measures taken to deny unauthorized persons information derived from telecommunications and to ensure the authenticity of such telecommunications. Note: Communications security includes cryptosecurity, transmission security, emission security, and physical security of COMSEC material and information.

Compromise

The disclosure of sensitive data to persons who are not authorized to receive such data.

Computer

A machine capable of accepting, performing calculations on, or otherwise manipulating or storing data. A computer usually consists of arithmetic and logical units and a control unit, and it may have input and output devices and storage devices.

Computing Environment

The total environment in which an IT system operates. The environment includes not only physical, administrative, and personnel procedures but also communication and networking relationships with other information systems.

Confidentiality

Assurance that information is not disclosed to unauthorized persons, processes, or devices.

Configuration Control

The process of controlling modifications to hardware, firmware, software, and documentation to ensure that the information system is protected against improper modifications before, during, and after system implementation.

Configuration Control Board

The CCB is a committee that has the final authority over all proposed changes to the IT system. The CCB discusses proposed changes, configuration status reports, and other topics that may be of interest to the different areas of the system's development. The board controls changes to the system and ensures that only approved changes are implemented in the system. It carries out this function by considering all proposals for modifications and new acquisitions and by making decisions regarding them. Once a decision has been reached regarding any modifications, the CCB is responsible for prioritizing the approved modifications to ensure that those that are most important are developed first. The CCB is responsible for assigning an authority to perform the change and for ensuring that the configuration documentation is updated properly. During the development of any enhancements and new developments, the board continues to exert control over the IT system by determining the level of testing required for all developments. The CCB is responsible for verifying that the changes have been properly incorporated and that only the approved changes have been incorporated. The board will review the test results of any developments and should be the final voice on release decisions. The membership of the CCB should include the bureau Chief Information Officer (CIO), DAA, Information Systems Security Manager (ISSM), and program official. Other individuals may be called upon to respond to issues that are brought to the board.

Configuration Management

Management of security features and assurances through control of changes made to hardware, software, firmware, telecommunications, documentation, test, test fixtures, and test documentation throughout the development and life cycle of the IT.

Contingency Management

Management of all the actions to be taken before, during, and after a disaster (emergency condition), along with documented, tested procedures, which if followed, will ensure the availability of critical IT systems and will facilitate maintaining the continuity of operations in an emergency situation.

Contingency Plan

The interim measures to recover IT services following an emergency or a system disruption.

Contracting Officer

Treasury officials with authority to enter into and administer contracts and make determinations and findings regarding pre-contract, contract award, and post-contract stages of a contract.

Contractor

Any industrial, educational, commercial, or other entity that has executed a contract with a Treasury bureau for performing a contract. The term also refers to an individual who manages such an entity.

Control Objectives

A statement of intent with respect to the oversight of some aspects of an organization's resources or processes, or both. In terms of IT systems, control objectives provide a framework for developing a strategy for fulfilling security requirements for any given system. The three basic control objectives for securing IT systems are security policy, accountability, and assurance.

Corrective Action

An action taken at the time an observation is made or thereafter that brings the situation into compliance with policy.

Countermeasure

An action or a device, procedure, technique, or other measure that reduces the vulnerability of an IT system.

Criminal Threat

A domestic adversary who has the capability and intent to access Treasury information in an IT system for purposes of conducting or aiding unlawful activities (i.e., fraud, smuggling, murder, technology transfer). Terrorist or technology transfer activities and other crimes carried out by a foreign government or person(s) fall under foreign threat.

Critical Resources

Those physical and information assets required for the performance of the site mission.

Cryptoperiod

The time span during which each key setting remains in effect.

D

Data

A representation of facts, concepts, information, or instructions suitable for communication, interpretation, or processing by humans or by an IT system.

Data Communications

A general data processing term that refers to communications among computers. Data communications, a component of telecommunications associated with IT, is included within the scope of this publication and will generally make use of telecommunications systems and/or facilities that may have been separately accredited under other national plans. (See also *Associated Data Communications.*)

Data Encryption Standard (DES)

A cryptographic algorithm for the protection of unclassified data and published by the National Institute of Standards and Technology (NIST) in FIPS PUB 46.

Data Integrity

The condition existing when data is unchanged from its source and has been neither accidentally nor maliciously modified, altered, or destroyed.

Data Owner

The authority, individual, or organization that has original responsibility for the data by statue, Executive order, or directive.

Deficiency

A security noncompliance situation that is of such a nature that significant damage or major inconvenience would result if acted on by a threat. It may also be a noncompliance situation in which a potential threat has no intervening safeguards or countermeasures to prevent it from acting directly on a vulnerability.

Degausser

A device that can generate a magnetic field for degaussing magnetic storage media.

Degaussing

A procedure that reduces the magnetic flux to zero by applying a reverse magnetizing field. Also called demagnetizing.

Demilitarized Zone (DMZ)

A network located between internal and external networks that has only two access points. It is usually used to isolate data for checking before allowing passage to the protected network. For example, a DMZ could be located between an Internet connected router and a bastion host.

Denial of Service (DoS)

The result of any action or series of actions that prevents any part of a secure telecommunications or IT system from functioning.

Designated Accrediting Authority

The official who has the authority to decide on accepting the security safeguards prescribed for an IT or the official who may be responsible for issuing an accreditation statement that records the decision to accept those safeguards. For classified IT, the DAA shall be the head of a bureau or a deputy assistant secretary-level official within departmental offices (DO). For sensitive IT, the DAA of such systems shall be based on managing a U.S. Treasury or bureau mission or function supported by IT or have authority to evaluate the overall mission requirements of the IT or network. DAAs shall have authority to evaluate the overall mission requirements of the IT and to provide definitive directions to IT developers or owners relative to the risk in the security posture of the IT.

Destruction

The physical alteration of IT media or of IT components such that they can no longer be used for storage or retrieval of information.

Direct User (*also referred to as a directly connected user*)

A user who is electronically connected to an IT typically via an interactive link and whose access is automatically limited in real time by the IT on some basis (e.g., security clearance, need to know).

The directly connected user has access to the various capabilities of an IT (e.g., databases, programs, and system output) and interacts with the IT in near real time. In addition to protecting the data processed on the IT from inadvertent system spillage and misroutes, the IT must provide adequate near-real-time controls to limit the direct user's access to those processing capabilities for which the user has been authorized and to withstand potential direct attacks

against the system's security controls. The means of electronic connection for this type of user may include one or more of the following: a) a point-to-point link, b) a LAN, or c) a global network. There are no geographic restrictions regarding how far a directly connected user may be from the IT. A given computer system may have direct and indirect users. Direct users present a significantly higher risk of security compromise in an IT than do indirect users, who do not have interactive access to an IT. (See also *Indirect User*.)

Disaster Recovery Planning

The process of developing advance arrangements and procedures that will enable an organization to respond to a disaster and resume its critical business operations within a predetermined period of time, minimize the amount of loss, and repair the stricken facilities as soon as possible.

E

Electronic Funds Transfer (EFT) Wire Transaction

The movement of value from one party to another by electronic means. This process excludes physical media transfers by magnetic tape, cartridge, diskette, or other similar technology.

Electronic Mail Message

A document created or received on an e-mail system, including brief notes, more formal and substantive documents, and any attachments, such as word processing documents transmitted, but not created, on an e-mail system.

Electronic Record

Any information that is recorded in a form that only a computer can process.

Employee Nonwork Time

The time when the employee is not otherwise expected to be addressing official business. Employees may, for example, use government office equipment during their own off-duty hours, such as before or after a workday (subject to local office hours), lunch periods, authorized breaks, or weekends or holidays if their duty station is normally available at such times.

Encryption Algorithm

A set of mathematically expressed rules for rendering data unintelligible by executing a series of conversions controlled by a key.

Environmental Threat

Any surrounding unintentional or natural accident, incident, or malfunction that may cause damage to IT resources, information, and personnel (i.e., structural failure, power fluctuation, temperature/humidity fluctuation, and heating and cooling system failure).

Erasure

A process intended to render magnetically stored data irretrievable by normal means.

External Network

Any network residing outside the security perimeter established by the firewall system.

Extranet

A private network segment providing limited connectivity between a completely nonpublic intranet and outside partners or the public Internet.

F

Facility

A physically definable area consisting of a controlled space that contains national security or sensitive information processing equipment.

Federal Bridge Certification Authority

A federal CA established to support interoperability among federal agency Public Key Infrastructure (PKI) domains.

Federal EFT System

A system owned, rented, or leased by the U.S. Government to process EFT data.

Field Review

The review of the technical and nontechnical security features employed by a system within its operational environment to ensure that the provisions of this security handbook are implemented. Field reviews may include penetration testing and are often used to certify to the accrediting authority that appropriate security measures have been implemented to protect the information processed within an acceptable level of risk.

File Transfer Protocol

A Transmission Control Protocol used to transfer files from a server to a client.

Firewall

System components (e.g., gateway, bridge, router, or front-end processor) that limit access between networks in accordance with local security policy.

Foreign Threat

The extant military, economic, and political capabilities of a foreign nation or person(s) coupled with the aggressive determination to use such capabilities to undertake any action whose consequence would be detrimental to the United States or the Treasury mission.

G

Gateway

Interface providing compatibility between networks by converting transmission speeds, protocols, codes, or security measures.

Gauss

A unit measure of the magnetic flux density produced by a magnetizing force.

General Records Schedules (GRS)

Mandatory disposition instructions issued by the National Archives and Records Administration (NARA) for temporary administrative records that are common to most federal agencies. (See, also *Record Schedule.*)

General Support System

An interconnected set of information resources, under the same direct management control, that share common functionality. A system normally includes hardware, software, information, data, applications, communications, and people. A system can be, for example, a LAN, including smart terminals that support a branch office; an agencywide backbone; a communications network; a departmental data processing center, including its operating system and utilities; a tactical radio network; or a shared information processing service organization.

Government Office Equipment, Including Information Technology

Includes personal computers and related peripheral equipment and software, library resources, telephone services, fax machines, photocopiers, office supplies, Internet connectivity and access to Internet services, and e-mail, but excludes the use of franked or official envelopes, mailing labels, or endorsements authorized by law.

H

Human Threat

A person or an organization with the capability and intention to do damage to the Treasury mission.

Hypertext Transfer Protocol

A Transmission Control Protocol used to transfer hypertext documents from a server to a client.

I

Identification

The process an information system uses to recognize an entity.

Indirect Users (*also referred to as indirectly connected users*)

In contrast to a direct user, an indirect user receives system output produced outside his or her control either a) by an automatic mechanism within the IT or b) from a process initiated by a direct user. An indirect user is precluded from initiating a process on the IT *and* receiving the output there from.

An indirect user is one who is electronically connected to an IT by other than a direct, interactive link. An IT that supports indirect users does not have to withstand direct attacks against the system's security controls because an intervening process between the indirect user and the IT affords some protection and control. The IT must protect the processing capabilities of the IT from inadvertent system spillage and misroutes and generally provides some control over indirectly connected users who may attempt to gain unauthorized access to the processing capabilities of the IT. Although there are a wide range of security risks associated with this type of user, these risks are not considered to be as significant as those associated with directly connected users. As with a direct user, the means of electronic connection for this type of user may include one or more of the following: a) a point-to-point link, b) a LAN, or c) a global network. There are no geographic restrictions as to how far an indirectly connected user may be from the IT.

Indirect users of an IT also include those who receive system output that has been generated electronically on the IT and is forwarded to a user without first undergoing a reliable human review of the data to determine whether it is appropriately classified and marked (e.g., to protect against system spillage and misroutings). Examples of indirect users include those who receive (without a reliable human review) printed output, and floppy or hard disks.

Individual Accountability

Requires individual users to be held accountable for their actions after being notified of the Rules of Behavior in using the system and the penalties associated with the violation of those rules.

Information

The terms data, information, material, documents, and matter are considered synonymous and used interchangeably in this manual. They refer to all data regardless of its physical form (e.g., data on paper printouts, tapes, disks, or disk packs; in memory chips; in random access memory [RAM]; in read only memory [ROM]; on microfilm or microfiche; on communication lines; and on display terminals).

Information Assurance

Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Information Owner

An individual responsible for establishing the rules for appropriate use and protection of the data/information. The information owner retains that responsibility, even when the data/information is shared with other organizations.

Information Systems Security Manager (ISSM)

The individual who will serve the bureau CIO as the principal advisor on computer security matters and who is responsible for developing and overseeing the bureau IT security program.

Information Systems Security Officer

An individual formally appointed by the program official to ensure that the provisions of all applicable directives identified within the scope of this handbook are implemented throughout the life cycle of each IT. ISSOs should be involved with an IT from the beginning of the concept development phase through its design, development, operation, maintenance, and secure disposal. ISSOs or, if appropriate, the available security staff must be identified in the accreditation documentation. An individual may be the ISSO for more than one IT system.

Information Technology

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.

Information Technology Facility

One or more rooms, generally contiguous, containing the elements of an IT system.

Information Technology Security

The protection of information systems against unauthorized access to or modification of information, whether in storage, processing, or transit, and against the DoS to authorized users, or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats.

Integrity

Quality of an IT system reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. Note that, in a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information.

Interim Authority to Operate

The system does not meet the requirements as stated in the system security authorization agreement, but mission criticality mandates that system become operational. It is a temporary approval that may be issued for no more than a 6-month period with one extension.

Interim Security Features and Measures

The security features provided by an IT that cannot be retrofitted with trusted products identified on the Common Criteria Products List until resources and/or technology developments make their use feasible. Interim security features include security-related hardware and/or software that is incorporated into key components of an IT or network (e.g., hardware, operating systems, extensions to operating systems, database management systems, specialized applications software, personal identification and verification devices, data encryption/encoding devices or software, and auditing tools). In addition, automated guard processes (or processors) or security filters may be used as interim features.

Internal Network

A network configured exclusively for Department use and managed by a departmental bureau.

Internal Threat

A primary threat to all information systems is one posed by individuals who are allowed authorized access to the system, but who intentionally or unintentionally exploit or abuse their access resulting in the compromise of data, degradation of system performance, or disruption of system services.

Internet

A loose confederation of networks around the world, the networks that make up the Internet are connected through several backbone networks. The Internet grew out of the U.S. Government ARPAnet project, and is specifically designed to have no central governing authority or "root" node.

Internet Control Message Protocol

A low-level mechanism used to influence the behavior of Transmission Control Protocol and User Datagram Protocol (UDP) connections. Supports the ping program.

Intranet

A private network using standard Internet protocols but with limited or no connectivity to the public Internet. An intranet is often connected to the public networks via a firewall.

IT Security Incident

Attempted or actual compromise of the confidentiality, integrity, or availability of a computer system or its information.

J

Java

A programming language developed by Sun Microsystems.

JavaScript

A scripting language developed by Netscape Corporation.

Java Security Model

An architecture that imposes security restrictions on local Java code and code obtained from a network connection. Java code when executed from a browser should not be able to read or write files on the client system or establish a network connection to a site other than the site from which the code was downloaded. Information can be obtained from Sun at URL http:java.sun.com/sfaq/#prevent.

Joint Accreditation

An accreditation process that is required when an IT or network processing sensitive data is not under the sole jurisdiction of a single accrediting authority. This often occurs when an IT or a network is used for processing various levels of sensitive data or when such systems are under the cognizance of more than one accrediting authority.

Systems processing Treasury information will require a joint accreditation with an appropriate Treasury official when such systems are under the operational control of a U.S. Government official not connected with the Department of the Treasury.

K

Key

Information used initially to set up and periodically change the operations performed in cryptographic equipment for encrypting and decrypting electronic signals.

Keying Material

A sequence of symbols or their electrical or mechanical equivalents which, in machine or auto-manual crypto systems, is combined with plaintext to produce ciphertext.

Key Management

Process by which key is generated, stored, protected, transferred, loaded, used, or destroyed.

Key Management Plan

A strategy that addresses how keying material will be generated, stored, protected, transferred, loaded, used, and destroyed. The plan includes format of key, cryptoperiod, forecasting quantitative requirements, and classification and sensitivity of keying material. A key management plan is concerned with systems security, physical security, personnel security, interoperability, manageability, and user friendliness.

L

Label

The marking of an item of information to reflect its security classification.

a. **Internal Label.** The marking of an item of information to reflect the classification of the information within the confines of the medium containing the information.

b. **External Label.** The visible and readable marking on the outside of the medium or the cover of the medium that reflects the classification of the information resident within the medium.

Least Privilege

The principle requiring that each subject be granted the most restrictive set of privileges needed for the performance of authorized tasks. Application of this principle limits the damage that can result from accident, error, or unauthorized use of an IT system.

Limited Official Use

See *Department of the Treasury Security Manual*, Chapter III, Section 2.

Limited Personal Use

The use of government-owned equipment by employees during personal time is considered an "authorized use" because the term is used in the Standards of Conduct for Employees of the Executive Branch [5 CFR § 2635.101 (b) (9) and § 2635.704 (a)]. Employees are specifically prohibited from the pursuit of private commercial business activities for profit-making ventures using the Government's office equipment. The ban also includes an employee's using the Government's office equipment to assist relatives, friends, or other persons in such activities (e.g., employees may not operate or participate in operating a business with the use of the Department's computers and Internet resources).

Logic Bomb

A resident computer program triggering an unauthorized act when particular states of an IT are realized. For example, a specific social security number in a payroll system is processed and the logic bomb is activated, resulting in an improper amount of money being printed on the check.

M

Machine-Readable Media

Media that can convey data to a given sensing device (e.g., diskettes, disks, tapes, and computer memory).

Major Application

An application that requires special attention to security because of the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Note: All federal applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight and should be treated as major. Adequate security for other applications should be provided by the security of the systems in which they operate.

Malicious Software

Any of a family of computer programs developed for the sole purpose of doing harm. Malicious code is usually embedded in software programs that appear to provide useful functions but, when activated by a user, cause undesirable results.

Material Weakness

Management control weaknesses that pose a risk or a threat to the internal control systems of an audited entity, such as a program or operation. A control weakness should be considered material, and therefore reportable, if the absence of the control results in failure to provide reasonable assurance that the control objectives will be met.

Minimal Additional Expense

Means that the employee's limited personal uses of government office equipment is limited to those situations in which the Government is already providing equipment or services. The employee's use of such equipment or services will not result in any additional expense to the Government or will result only in normal wear and tear or the use of small amounts of electricity, ink, toner, or paper. Examples of minimal additional expenses include making a few photocopies, using a computer printer to print out a few pages of material, making occasional brief personal phone calls, infrequently sending personal e-mail messages, or limited use of the Internet for personal reasons.

Mission-Critical Information

Information that must be protected from loss or disclosure to keep an adversary or competitor from gaining a significant operational, economic, political, or technological advantage and prevent adverse impact on a classified or unclassified mission accomplishment.

N

National Security Systems

Those telecommunications and ITs operated by the U.S. Government, or its contractors or agents, that contain classified information or that involve intelligence activities, cryptologic activities related to national security, command and control of military forces, equipment that is an integral part of a weapon or weapons system, or equipment that is critical to the direct fulfillment of military or intelligence missions.

Natural Threat

A threat posed by fire or natural disasters such as tornado, earthquake, or flood.

Need to Know

The necessity for access to, or knowledge or possession of, specific information required to carry out official duties.

Network

Comprises communications media and all components attached thereto whose responsibility is the transfer of information among a collection of IT systems or workstations. Network components include packet switches, front-end computers, network controllers, technical control devices, and other networks. In the context of this handbook, such networks a) are under the operational control of a Treasury official, b) are used for the transmission of classified or sensitive data, and c) may provide connectivity among IT systems operated by various classified or sensitive information components. Networks include wide- and local-area technologies.

Nonrepudiation

Nonrepudiation provides the sender with proof of delivery and the recipient with proof of the sender's identity, so that neither can later deny having processed the data.

O

Observation

A general term that denotes a situation and/or circumstances that are not in compliance with established security policies.

On-the-Spot Correction

Actions taken that totally correct a situation observed and bring it into compliance before a review team concluding its exit briefing at a reviewed site.

Operational Controls

Operational controls address security methods that focus on mechanisms that primarily are implemented and executed by people (as opposed to systems).

Other Threats

The capability and intent of sources, human or otherwise, that can cause harm to Treasury's mission. Threats that are not foreign or criminal include natural disasters, environmental threats, or human threats that are not related to criminal activities (e.g., unintentional errors or an insider who abuses systems without committing a criminal act).

P

Packet Filtering

The process of screening Internet Protocol (IP) packets based on some combination of the source IP address, destination IP address, UDP source port, UDP destination port, and incoming network interface.

Password

A protected/private alphanumeric string used to authenticate an identity or to authorize access to data.

Password Space

The total number of possible passwords that can be created by a given password generation scheme.

Perimeter of a System

The perimeter of a system encompasses all those components of an IT or network that are to be accredited. As a rule, separately accredited components are not included within the perimeter—those components are within the boundary.

Personnel Security

The procedures established to ensure that all personnel (employees and contractors) who have access to any sensitive or classified information have had the necessary personnel investigation completed on them, have the required authorizations, and have been granted appropriate security background clearances and have a need to know.

Personnel Security Clearance

An administrative determination that an individual is eligible from a security point of view for access to classified information of the same category as, or lower category than, the level of the personnel security clearance being granted.

Physical Destruction Threat

The threat of terrorist attack on Treasury must be rated high. The political climate worldwide varies from day to day, with attempted assaults on data a fairly routine occurrence. A physical destruction threat is an event of catastrophic proportions that destroys the building or facility or renders it inoperable.

Physical Security

a. The use of locks, guards, badges, alarms, procedures, and similar measures (alone or in combination) to control access to the IT system and related equipment.

b. The measures required for the protection of the structures housing the IT, related equipment, and their contents from espionage, theft, waste, fraud, abuse, or damage by accident, fire, and environmental hazards.

Program Manager

The individual who is ultimately responsible for the overall procurement, development, integration, modification, or operation and maintenance of the IT system.

Program Official

A division director, or equivalent, who is responsible for a major program or functional area.

Proxy

An application running on a firewall that relays requests/communication from client/server software running on an internal network to client/server software located on an external network.

Purge

Render stored data unrecoverable by laboratory attack.

R

Records

Includes all books, papers, photographs, machine-readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the U.S. Government under federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of data in them.

Record Schedule

A document that describes agency records, establishes a period for their retention by the agency, and provides mandatory instructions for what to do with them when they are no longer needed for current government business. The term means a) a Standard Form (SF) 115, Request for Records Disposition Authority, that has been approved by NARA to authorize the disposition of federal records; b) a GRS issued by NARA; or c) a printed agency manual or directive containing the records descriptions and disposition instructions approved by NARA of one or more SF 115s or issued by NARA in the GRS.

Registration Authority

An agent of a CA that collects information used to generate a digital certificate.

Relying Parties

An entity that uses PKI services to implement applications.

Remote Access Feature

A feature that permits authorized callers from the public network to access the system and use its features and services.

Reportable Condition

This includes matters coming to the auditor's attention that, in the auditor's judgment, should be communicated because they represent significant deficiencies in the design or operation of internal controls that could adversely affect the entity's ability to properly report financial data.

Residual Risk

A portion of risks remaining after security measures have been applied.

Risk

A combination of the likelihood that a threat shall occur, the likelihood that a threat occurrence shall result in an adverse impact, and the severity of the resulting adverse impact.

Risk Analysis

Synonymous with risk assessment.

Risk Assessment

Process of analyzing threats to and vulnerabilities of an information system, and the potential impact that the loss of information or capabilities of a system would have on national security, and using the analysis as a basis for identifying appropriate and cost-effective countermeasures.

Risk Management

The process concerned with the identification, measurement, control, and minimization of security risks in IT to a level commensurate with the value of the assets protected.

Root

The most trusted CA in a hierarchical x.509-based PKI.

Rules of Behavior

Rules of Behavior are the rules that have been established and implemented concerning use of, security in, and acceptable level of risk for the system. Rules will clearly delineate responsibilities and expected behavior of all individuals with access to the system. Rules should cover such matters as work at home, dial-in access, connection to the Internet, use of copyrighted works, unofficial use of federal government equipment, assignment and limitation of system privileges, and individual accountability.

S

Sanitization

The elimination of sensitive or classified information from an IT system or media associated with an IT system to permit the reuse of the IT or media at a lower sensitivity or classification level or to permit the release to uncleared personnel or personnel without the proper need-to-know authorizations.

Scan

To examine computer coding and programs sequentially, part by part. For viruses, scans are made for virus signatures or potentially unsafe practices (e.g., changes to an executable file, direct writes to specific disk sectors).

Secure Area

A physically defined space containing classified matter (documents or material) subject to physical protection and personnel access controls.

Secure Telephone Equipment

A secure telephone unit that has been endorsed by the National Security Agency (NSA) for securing classified or sensitive U.S. government information when appropriately keyed.

Security

The measures and controls that ensure confidentiality, integrity, availability, and accountability of the information processed and stored by a computer.

Security Event

An occurrence in a system that is relevant to the security of the system.

Security Features

The security-relevant functions, mechanisms, and characteristics of IT hardware and software (e.g., identification and authentication, audit trail, access control).

Security Incident

An attempt to exploit an information system such that the actual or potential adverse effects may involve fraud, waste, or abuse; compromise of information; loss or damage of property or

information; or denial of service. Security incidents include technical and administrative vulnerabilities, and introduction of computer viruses or other forms of malicious code.

Security Incident Response

Actions conducted to resolve information systems security incidents and protect national security systems.

Security Product

A product (e.g., software, hardware, or combination) with the primary function or purpose of providing features or capabilities to implement protective and detective measures, controls, or safeguards.

Security Safeguards

The protective measures and controls that are prescribed to meet the security requirements specified for an IT system. Safeguards may include, but are not necessarily limited to, hardware and software security features; operation procedures; accountability procedures; access and distribution controls; management constraints; personnel security; and physical structures, areas, and devices.

Security Test and Evaluation

The examination and analysis of the safeguards required to protect the information system as they have been applied in an operational environment, to determine the security posture of that system.

Security Violation

A failure to comply with policy and procedures established by the Federal Government that reasonably could result in the loss or compromise of sensitive information.

Sensitive Information

Any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest, the conduct of federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, United States Code (U.S.C.) (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive order or an act of Congress to be kept secret in the interest of national defense or foreign policy. This definition is synonymous with Sensitive Information as defined in Public Law 100-235, The Computer Act of 1987, dated January 8, 1988. In addition, Treasury sensitive information includes trade secret or confidential information protected by Section 1905 of Title 18, U.S.C. (The Trade Secrets Act). All information designated Limited Official Use is included within sensitive information.

Sensitivity

The IT environment consists of the system, data, and applications that must be examined individually and in total. All systems and applications require some level of protection for confidentiality, integrity, and/or availability that is determined by an evaluation, of the sensitivity of the information processed, the relationship of the system to the organization's mission, and the economic value of the system components.

Server Side Includes

Directives included in hypertext documents that evoke program and/or command execution on a server.

Set of Accredited Security Parameters

The set of security classification level(s) at which an IT system is accredited to operate. The Set of Accredited Security Parameters (SASP) will reflect the type(s) of data that the accrediting authority believes the system can reliably keep segregated within an acceptable level of risk in the context of the particular security mode of operation.

The SASP of an IT system with respect to a particular network connection is the set of the different type(s) of data that the IT system can legitimately transmit to or receive from the network. Dedicated and system-high mode IT systems have a single accredited security parameter (e.g., Top Secret). The SASP for a multilevel mode system includes two or more levels of classified information (e.g., Confidential, Secret, and Top Secret) processed and reliably separated on the same system.

Significant Computer Security Incident

Any information security-related incident that slows or prevents the use of a computer, network, or system for longer than 30 minutes; impacts another bureau, agency, or organization; or impacts a Treasury critical asset.

Site

One or more operational facilities, usually geographically contiguous, operated by or for the Treasury under the management and administrative direction of a Treasury bureau or Treasury bureau contractor.

Subcontract

Any contract entered into by a contractor to furnish supplies, goods, or services for performance of a prime contract on a subcontract. Any contract, subcontract, purchase order, lease agreement, service agreement, request for quotation, request for proposal, solicitation, or other

agreement or procurement action between one or more contractors that requires access to classified information to fulfill the performance requirements of a prime contract.

Subcontractor

A supplier, distributor, vendor, or firm that furnishes supplies, goods, or services to or for a prime contractor or another subcontractor or who enters into a contract with a prime contractor.

Subscribers

Individuals who are issued certificates, sometimes referred to as subscribers in PKI references.

Suspected Computer Security Incident

An event that may not have caused a disruption of mission-essential processing by indications that a) a significant attempt to breach security occurred but proved unsuccessful or b) a significant leak or unauthorized access of data occurred but did not disrupt the computer application. The CIO should be contacted, although the likelihood of action in this instance is less certain.

System

The interconnected set of information resources under the same direct management control, which share common functionality. A system normally includes hardware, software, information, data, applications, communications, and people. A system can be, for example, a LAN, including smart terminals that support a branch office; an agencywide backbone, a communications network; a departmental data processing center, including its operating system and utilities; a tactical radio network; or a shared information processing service organization.

System Integrity

An attribute of an information system when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

System Operational Status

System operational status is either a) Operational—system is in operation, b) or Under Development—system is under design, development, or implementation, or c) Undergoing a Major Modification—system is undergoing a major conversion or transition.

System Security Authorization Agreement

A formal agreement among the DAA, certifier, information system user representative, and program manager. It is used to guide actions and to document decision, security requirements,

certification tailoring and level-of-effort, certification results, certifier's recommendation, and the DAA's approval to operate.

T

Technical Controls

Technical controls consist of hardware and software controls used to provide automated protection to the system or applications. Technical controls operate within the technical system and applications.

Technical Vulnerability

A hardware, firmware, or software weakness or design deficiency that leaves an information system open to potential exploitation, either externally or internally, thereby resulting in risk of compromise of information, alteration of information, or DoS.

Telecommunications

Preparation, transmission, communication, or related processing of information (writing, images, sounds, or other data) by electrical, electromagnetic, electromechanical, electro-optical, or electronic means.

Threat

Any circumstance or event with the potential to harm an IT system through unauthorized access, destruction, disclosure, modification of data, and/or DoS.

Threat Assessment

Formal description and evaluation of threat to an information system.

Time Bomb

Resident computer program that triggers an unauthorized act at a predefined time. The "Friday the 13th" computer virus is an example. This virus infects the system several days or even months before and lies dormant until the date reaches Friday the 13th.

Trap Door

Hidden software or hardware mechanism used to circumvent security controls. Synonymous with back door.

Transmission Control Protocol/Internet Protocol

A collection of communications protocols spanning the network and transport layers of the Open Systems Interface seven-layer protocol model. The main components are the Transmission Control Protocol, which provides virtual circuits to the user, and the IP, which functions at the transport layer providing IP addresses.

Treasury Critical Infrastructure

Critical infrastructures are those Treasury IT systems, facilities, personnel, and physical assets used to perform critical national and sector-related law enforcement and banking/financial functions by the Department and its bureaus. If any of these assets were destroyed or incapacitated, the result would be a debilitating national or regional impact in terms of public health and welfare, economic well-being, public confidence and governance, and national defense.

Treasury System

An IT system (e.g., telecommunications, networks, computers, and applications) that is a) owned, leased, or operated by a bureau, DO, Office of the Inspector General (OIG), Treasury Inspector General for Tax Administration (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.

Trojan Horse

Program containing hidden code allowing the unauthorized collection, falsification, or destruction of information.

Two-Person Control

The close surveillance and control of certain materials at all times by a minimum of two appropriately authorized individuals. Each individual shall be capable of detecting incorrect and unauthorized procedures with respect to the tasks to be performed and shall be familiar with established security requirements.

Type I

Classified or controlled cryptographic product endorsed for securing classified or sensitive U.S. government information when appropriately keyed.

Type II

Unclassified cryptographic device or equipment endorsed for protecting sensitive U.S. government or government-derived information.

U

Unauthorized Disclosure

Exposure of information to individuals not authorized to receive it.

Usenet

Worldwide public conferencing network accessible from the Internet.

User

Person or process authorized to access an IT system.

User Datagram Protocol

A connectionless transport protocol that extends to the application level the same services as IP. This protocol does not provide for error correction or fault tolerance.

V

Validation

A process of applying specialized security test and evaluation procedures, tools, and equipment needed to establish acceptance for joint usage of an IT system by one or more departments or agencies and their contractors.

Verification

The process of comparing two levels of an IT system for proper correspondence (e.g., security policy model with top-level specification, top-level specification with source code, or source code with object code).

Virtual Private Network

Any one of a number of tunneling protocol variations. This capability provides protected communications over inherently nonsecure networks. Some variations extend the protected service from user to user or firewall to firewall.

Virus

Self-replicating, malicious program segment that attaches itself to an application program or other executable system component and leaves no obvious signs of its presence.

Virus Detection Software

Software written to scan machine-readable media on computer systems. A growing number of reputable software packages are available that are designed to detect and/or remove viruses. In addition, many utility programs can search text files for virus signatures or potentially unsafe practices.

Virus Signature

A unique set of characters that identify a particular virus. This may also be referred to as a virus marker.

Vital Records

Records that are identified, duplicated, and stored off premises in a suitable environment located a safe distance from the office or bureau. Each DO and each bureau is responsible for sending vital records to and retrieving them from the off-premises storage facility using reliable packing methods and transport mechanisms that guarantee delivery and safe storage of vital records. Frequency of shipping correlates directly with the recovery objectives of the DO or bureau.

Vulnerability

A weakness in an IT system or cryptographic system or system security procedures, hardware design, or internal controls that could be exploited in attempting to gain unauthorized access to classified or sensitive information.

Vulnerability Assessment

The systematic examination of an IT system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

W

World Wide Web

Distributed heterogeneous document and multimedia information system based on standard protocols and accessible from the Internet.

Worm

Independent program that replicates from machine to machine across network connections, often clogging networks and computer systems as it spreads.

X

X.509

A widely used standard for defining digital certificates developed by the International Telecommunications Union.

APPENDIX A—TCSIRC CONTACT INFORMATION

TCSIRC can be contacted by telephone, fax, and e-mail or through an online Web portal. As of August 1, 2002, Booz Allen Hamilton and NETSEC support the TCSIRC, with NETSEC providing the 24x7x365 reporting center.

CONTACT INFORMATION	
NETSEC 24x7 phone number	703-561-9042
NETSEC fax number	703-561-9178
NETSEC e-mail	nsoc@netsec.net
TCSIRC e-mail	tcsirc@do.treas.gov
Web portal (login required)	https://netsecintelligence.net

APPENDIX B—RESPONSE GUIDELINES

Incidents shall be prioritized and handled accordingly. As additional information becomes available, the priority and criticality of the incident may change. Common sense, knowing when to escalate an incident, and the ability to reprioritize are critical incident handling skills for an incident handler at both the bureau and the Department levels. Exhibits B-1 and B-2 provide the initial response for each incident type required to be reported to the TCSIRC.

Exhibit B-1. Minor Incident Response Guidelines

Bureau CSIRCs are not required to report minor incidents to the TCSIRC on an incident basis. Minor incidents should be rolled up into a monthly summary report provided to the TCSIRC.

Misuse of Resources
Identify the misuse of the computing or telecommunications system or network and determine whether the misuse resulted in any adverse impacts on the system. As required, follow appropriate incident handling guidelines, commensurate with the severity of the incident. Report the misuse of resources in the bureau's monthly summary report.
Loss or Theft of Equipment With Unclassified Information
Identify data that could be compromised, stolen, or lost with loss or theft of the equipment. Mitigation strategies and precautionary measures will vary. As required, follow appropriate incident handling guidelines, commensurate with the severity of the incident. Report the loss or theft of the equipment in the bureau's monthly summary report.
Probes and Reconnaissance Scans
Probes and reconnaissance scans may indicate that the network is being targeted for an attack. As required, follow appropriate incident handling guidelines, commensurate with the severity of the incident. Report probes or reconnaissance scans in the bureau's monthly summary report.
Unsuccessful Access and Penetration Attempts
Determine the source (e.g., IP address, brute force attack with a user ID) and targeted resource for the unsuccessful attempts. As required, follow appropriate incident handling guidelines, commensurate with the severity of the incident. Report unsuccessful access or penetration attempts in the bureau's monthly summary report.
Malicious Code Detection
Disinfect and contain the malicious code to prevent further spreading. As required, follow appropriate incident handling guidelines, commensurate with the severity of the incident. Report detections of malicious code in the bureau's monthly summary report.

Exhibit B-2. Significant Incident Response Guidelines by Incident Type

Significant incidents shall be reported to the TCSIRC within 1 hour of incident identification. Within 4 hours of incident identification, the bureau CSIRC shall provide a more detailed report. The guidelines in Exhibit B-2 provide the initial response to each significant incident type. Each bureau CSIRC shall determine appropriate incident handling guidelines, commensurate with the severity of the incident, to ensure that the incident is contained.

Unauthorized Alteration or Compromise of Data
Establish what information may have been altered or compromised, and then determine how this may have been done. Follow appropriate incident handling guidelines, commensurate with the severity of the incident. Notify the TCSIRC within 1 hour of identification of an alteration or compromise of the data.
Classified Incident
Classified incidents shall be reported to the TCSIRC for reporting to the NSIRC. Ensure that the reporting method is secure.
Denial-of-Service Attacks
Work with internet service provider to block the attacking IP address or coordinate defensive action with network operations. Follow appropriate incident handling guidelines, commensurate with the severity of the incident. Notify the TCSIRC within 1 hour of identification of a denial-of-service attack.
Domain Name System (DNS) Attack
Identify the targeted resource and source of the attack. Follow appropriate incident handling guidelines, commensurate with the severity of the incident. Notify the TCSIRC within 1 hour of identification of a DNS attack.
Loss or Theft of Equipment With Classified Information
Identify data that could be compromised, stolen, or lost with loss or theft of equipment. Mitigation strategies and precautionary measures will vary. Report lost equipment to the TCSIRC within 1 hour of acknowledgment that equipment is lost or stolen.
Successful Malicious Code Infections (not detected by antivirus software)
Disinfect infected files and disks; determine the damage and the source. Determine whether any information was compromised, and attempt to identify IP/individual gathering information. Follow appropriate incident handling guidelines, commensurate with the severity of the incident. Report any successful malicious code infections or identification of a new malicious code to the TCSIRC within 1 hour of identification.
Root Compromise
Disconnect compromised machine from the network to ensure that trusted machines do not become compromised. Follow appropriate incident handling guidelines, commensurate with the severity of the incident. Notify the TCSIRC within 1 hour of identification of a root compromise.

Unauthorized Access
Determine which user ID was compromised, and what systems are at risk. Follow appropriate incident handling guidelines, commensurate with the severity of the incident. Notify the TCSIRC within 1 hour of identification of successful unauthorized access.
Web Site Defacements
Determine what else has been impacted on the Web server and how the Web server was compromised. Notify the TCSIRC within 1 hour of identification of a Web site defacement.
Other
Report incidents, not defined in another incident type, that adversely affect a system. Response will vary with each incident. Follow appropriate incident handling guidelines, commensurate with the severity of the incident. Notify the TCSIRC within 1 hour of identification of an adverse mission impact.

.

APPENDIX C—TREASURY SECURITY INCIDENT REPORT FORM

THIS FORM IS FOR REPORTING INCIDENTS ON SENSITIVE BUT UNCLASSIFIED NETWORKS ONLY!
Please report classified incidents via secure communications.

Is this a CIP Asset? YES NO

Incident Site (Bureau Name, Acronym, and Location)

_____

_____

_____

Date and Time of Incident: **Priority Level: (1-5)**

Incident POC:
Name: _____
Email: _____
Phone: _____

Incident Type and Summary: (Please be as specific as possible. Include how incident was detected.)

System Information: (Please be specific, e.g., CIP Asset, version and patch level/Service Pack if applicable.)

Damage:
Downtime (hours) _____ Employees affected _____
Number of systems affected _____ Monetary value to repair _____
Loss of service to the public (Yes/No) _____

Cost:
☐ None ☐ Unknown ☐<$10K ☐$10K - $50K ☐ >$50K

APPENDIX D—SAMPLE BUREAU MONTHLY SUMMARY REPORT

Top 5 IP Addresses: (Report the five originating IP addresses that generated the most activity reported across all minor incidents)

Misuse of Resources: (Total number)

Loss or Theft of Equipment with Unclassified Information: (Total number)

Probes and Reconnaissance Scans: (Total number)

Unsuccessful Access and Penetration Attempts: (Total number)

Malicious Code Detection: (Total number of times malicious code was detected and cleaned by the antivirus software)

Other: (Description)

APPENDIX E—DEFINITIONS OF TREASURY SECURITY INCIDENTS

The following are security incidents and must be reported to the TCSIRC.

Minor Incidents:

a. **Misuse of Resources.** Mishandling by an authorized user of a computing or telecommunications system or network.

b. **Loss or Theft of Equipment With Unclassified Information.** Must be reported to the TCSIRC to determine the potential compromise of sensitive material. This includes the compromise of user accounts and passwords that could allow unauthorized persons to access Treasury computing resources, or agents' names or case information that could compromise an investigation or risk the loss of human life. The TCSIRC's emphasis is on the data that was lost or stolen, not the hardware itself.

c. **Probes and Reconnaissance Scans.** Include all suspicious probing or scanning of networks for critical services or security weaknesses.

d. **Unsuccessful Access and Penetration Attempts.** Include all suspicious unsuccessful access or penetration attempts, such as scans from Nimda or Code Red.

e. **Malicious Code Detection.** Include all malicious code detected.

Significant Incidents:

a. **Unauthorized Alteration or Compromise of Data.** Involve the unauthorized altering of information or incidents that result in a compromise of data.

b. **Classified Incident**. Involve a system used to process national security information or involve classified information on any system not certified for that level of classified information.

c. **Denial-of-Service Attacks.** Attacks that affect the availability of critical resources such as e-mail servers, Web servers, routers, gateways, or communications infrastructure.

d. **Domain Name System (DNS) Attack.** Attacks against the domain name system or protocol, such as DNS cache poisoning or spoofing.

e. **Loss or Theft of Equipment With Classified Information.** Must be reported to the TCSIRC to determine the potential compromise of sensitive material. This includes the compromise of user accounts and passwords that could allow unauthorized persons to access Treasury computing resources, or agents' names or case information that could compromise an investigation or risk the loss of human life. The TCSIRC's emphasis is on the data that was lost or stolen, not the hardware itself.

f. **Successful Malicious Code Infections (not detected by antivirus software).** Performed by attackers in an attempt to gain privileges and/or information, to capture passwords, and to modify audit logs to hide unauthorized activity. The attempts include the use of mobile code, such as viruses, Trojan horses, worms, and scripts. This category includes any code that is intended to disrupt or annoy users that was not detected and cleaned by the antivirus software.

g. **Root Compromise**. An intrusion in which the intruder has gained all privileges (including all security-related privileges) and thus can manage the system and its other user accounts.

h. **Unauthorized Access.** Includes all successful unauthorized access attempts.

i. **Web Site Defacements.** Superficial destruction of Web pages that could cause public embarrassment, but does not lead to an attack.

j. **Other.** Incidents that have significant impact on the mission of the site or operations but do not fall into any of the aforementioned categories.

Some bureaus are responsible for managing telecommunications systems and networks; those bureaus must also report incidents affecting those systems and networks.

APPENDIX F—GLOSSARY

Chain of Custody	Verifiable documentation that indicates the sequence of individuals that have handled a piece of evidence and the sequence of locations where that evidence has been stored, including dates and times. To ensure a verifiable chain of custody, the evidence must be accounted for at all times.
Classified System Incident	Any event that involves a system used to process national security information, a CIP Asset, or any discovery of classified information on any system not certified for that level of classified information (e.g., Secret information on a system not certified to process classified information; Top Secret information on a system certified only for processing Secret information).
Critical Infrastructure Protection	Critical infrastructures are those physical and cyber-based systems essential to the minimum operations of the economy and government. They include, but are not limited to, telecommunications, energy, banking and finance, transportation, water systems, and emergency services, both governmental and private.
Denial-of-Service	An attack that can consume all available memory and processor resources, thus rendering the router unusable.
Event	A notable occurrence, not yet assessed, in a computing or telecommunications system or network that may affect that system or network.
Incident	The violation of an explicit or implied security policy in a computing or telecommunications system or network.
Incident Handling	Actions taken to protect and restore the normal operating condition of computers and the information stored in them when an adverse event occurs; involves contingency planning and contingency response.
Incident Response	Same as incident handling.
Internal Incident	A bureau matter that has no impact on any other bureau, agency, or outside entity and does not require any law enforcement investigation.
Minor Incidents	A security-related incident classified as— • Misuse of resources • Loss or theft of equipment with unclassified information • Probe or reconnaissance scan • Unsuccessful access or penetration attempt • Malicious code detection.
Policy	A set of written statements directing the operation of an organization or community in regard to specific topics such as security or dealing with the media.
Procedure	The implementation of a policy in the form of workflows, orders, or mechanisms.
Significant Incidents	A security-related incident classified as— • Unauthorized alteration or compromise of data • Classified incident • Denial-of-service attack • Domain Name System attack • Loss or theft of equipment with classified information • Successful malicious code infection (not detected by antivirus software) • Root compromise • Unauthorized access • Web site defacement • Other (does not fit into a category above).
Triage	The process of collecting, sorting, recording, tracking, and prioritizing information to facilitate its appropriate handling.
Vulnerability	A weakness in a computing or telecommunications system or network, system security procedures, internal controls, or implementation that could be exploited.