





Information Security Program

Information Security Program Policy

July 19, 2005

SECURE ONE HHS

KEEP AMERICA'S HEALTH AND HUMAN SERVICES SECURE

Table of Contents

Preface

As the Department of Health and Human Services (HHS) Information Technology Security Program evolves, this document will be subject to review and update, which will occur annually or when changes occur that signal the need to revise the *HHS Information Security Program Policy*. These changes may include the following:

- Changes in roles and responsibilities;
- Release of new executive, legislative, technical, or Departmental guidance;
- Identification of changes in governing policies;
- Changes in vulnerabilities, risks or threats; and/or
- HHS Inspector General findings that stem from a security audit.

The HHS Chief Security Officer (CSO) must approve all revisions to the *HHS Information Security Program Policy*. Revisions are to be highlighted in the Document Change History table. Each revised policy document is subject to HHS' document review and approval process before becoming final. When it is approved, a new version of the *HHS Information Security Program Policy* will be issued, and all affected parties will be informed of the changes made.

Additionally, compliance with this document is *mandatory*. It is HHS policy that Department personnel abide by or exceed the requirements outlined in this document. In cases where an OPDIV or STAFFDIV cannot comply with the *HHS Information Security Program Policy* for technical or financial reasons, or because it precludes the OPDIV or STAFFDIV from supporting its mission or business function, justifications for the noncompliance shall be documented using the policy waiver form[1] and submitted to the appropriate OPDIV Chief Information Security Officer (CISO) for approval. Resulting risks from this deviation shall be documented in the appropriate risk management documentation.

1 Refer to appendix F for the policy waiver form.

Document Change History

Version Number	Release Date	Summary of Changes	Section Number/ Paragraph Number	Changes Made By
0.1	01/26/2004	Final Document Release	N/A	N/A
0.2	05/03/2004	Document Release with OIRM changes incorporated	Entire Document	HHS CSO
0.3	12/15/2004	Final Document Release with OPDIV changes incorporated	Entire Document	HHS CSO
0.4	07/19/2005	Update to reflect new HHS guidance and regulatory requirements.	Throughout	HHS CSO

1. Introduction

The United States Department of Health and Human Services (HHS) is responsible for implementing and administering an information security program. This program must protect the Department's information resources, in compliance with applicable public laws, federal regulations, and Executive Orders (E.O.), including the *Federal Information Security Management Act of 2002* (FISMA); the Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*, dated November 28, 2000; and the *Health Insurance Portability and Accountability Act of 1996* (HIPAA). To meet these requirements, HHS has instituted the *HHS Information Security Program Policy* and developed the accompanying *HHS Information Security Program Handbook*.

1.1 Scope and Applicability

This *HHS Information Security Program Policy* provides a baseline of security policies for the Department. These policies apply to the Department, which includes Operating Division (OPDIV) and Staff Division (STAFFDIV) personnel, contractors, and other authorized users. This document, and additional HHS guidance, provides a minimum standard for the Department. These standards will continue to be developed as the program matures. OPDIVs can exceed these standards, but must consistently apply *at least* the minimum.

This document establishes mandatory policies to ensure confidentiality, integrity, availability, reliability, and non-repudiation within the Department's infrastructure and its operations. It is the policy of HHS that the Department abides by or exceeds the requirements outlined in this document. In addition, to ensure adequate security, the OPDIVs shall implement additional security policies, as appropriate for their specific operational and risk environment. This policy supersedes the *HHS Automated Information Systems Security Program Handbook*, known as the *Redbook*, dated May 1994.

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

This *HHS Information Security Program Policy* imposes special responsibilities on some positions. These policies apply to all information systems, including hardware, software, and data, and to all facilities that house these information systems and infrastructures. The *HHS Information Security Program Handbook* provides additional details on implementing the policies stipulated in this document.

1.2 Authorities

The *Clinger-Cohen Act of 1996,* formerly the *Information Technology Management Reform Act* (Public Law 104-106), OMB Circular A-130, and FISMA are statutes that require federal agencies to protect their information resources and data by establishing information security programs and imposing special requirements for protecting personal information. This *HHS Information Security Program Policy* evolved from these mandates. It incorporates the requirements of E.O.s, Homeland Security Presidential Directives (HSPD), public laws, National Institute of Standards and Technology (NIST) Special Publications (SP), and federal and Departmental standards and regulations. This policy document will be used in conjunction with any current HHS Information Resource Management (IRM) policies and guidelines.

FISMA charges NIST with special responsibilities to develop guidance to improve federal-wide information security planning, implementation, management, and operation. Guidance from NIST's Computer Security Resource Center (CSRC) should be used to support the Department's information security efforts; instruction on a wide variety of information security related topics can be found at the NIST Web site, http://csrc.nist.gov/publications/index.html.

These authorities and guidance documents are listed in Appendix B.

2. Overview

This section provides an overview of this *HHS Information Security Program Policy*. It highlights the Department's information security policy requirements, security responsibilities, and summarizes subsequent sections of this document.

HHS is responsible for implementing a Department-wide information security program to assure that each information system and associated facility provides a level of security that is commensurate with the risk and magnitude of the harm that could result from the loss, misuse, disclosure, or modification of the information contained in the system. Each system's level of security shall protect the confidentiality, integrity, and availability of the information and comply with all security and privacy-related laws and regulations.

The Department shall administer an information security program that meets statutory, regulatory, and Departmental requirements, as well as the needs of the public. OPDIV information security programs shall comply with the HHS Information Security Program and must meet the minimum standards set forth by that program. OPDIVs may impose stricter policies where appropriate.

2.1 Document Organization

NIST delineates security controls into the three primary categories of management, operational, and technical, which structure the organization of the *HHS Information Security Program Policy* document.

- Section 3, Management Policies, focuses on the management of information security systems and the management of risk for a system. They are techniques and concerns that are normally addressed by management.
- Section 4, Operational Policies, addresses security methods focusing on mechanisms primarily implemented and executed by people (as opposed to systems). These controls are put in place to improve the security of a particular system (or group of systems). They often require technical or specialized expertise and often rely upon management activities as well as technical controls.
- Section 5, Technical Policies, focuses on security controls that the computer system executes. The controls can provide automated protection for unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data.[2]

This document contains policies that satisfy minimum-security requirements.

The *HHS Information Security Program Handbook* provides procedures outlining *how* to implement these policy requirements, and the HHS Information Security Program

2 Explanations from NIST SP 800-26, *Security Self-Assessment Guide for Information Technology Systems,* November 2001.

guides provide further guidance on specific aspects of the policy. (See Appendix E for a complete list of the HHS Information Security Program documents). These requirements satisfy FISMA and information security best practices.

2.2 Roles and Responsibilities

The HHS Information Security Program is a component of a larger structure. Congress and OMB have imposed special responsibilities on the HHS CIO and the HHS CSO, while still reinforcing the direct responsibilities of the Department's mission and business leaders. Ultimately, mission and business leaders remain responsible for using risk-management principles to select and implement appropriate information security safeguards. The infrastructure provided by the HHS CIO and supported by the HHS CSO and OPDIV CISOs supports these decisions.

The structure of the HHS Information Security Program is meant to provide collaboration between the OPDIVs and the HHS CIO, while assuring compliance with legislative and regulatory mandates and the *HHS Information Security Program Policy*. The program encompasses initiatives that address information security planning, policy development, education and awareness, communication, privacy, and compliance reviews. The program outlines individual responsibilities for specific roles within HHS. These individual responsibilities are explained in the following subsections.

2.2.1 Secretary of HHS

The Secretary for HHS is responsible for:

- Ensuring that an agency-wide information security program is developed, documented, and implemented to provide security for all systems, networks, and data that support operations of the Department;
- Ensuring that information security management processes are integrated with HHS strategic and operational planning processes;
- Protecting information systems and data by allocating resources in a manner consistent with risk;
- Ensuring that senior HHS officials provide information security for operations and information technology (IT) resources under their control;
- Delegating to the HHS CIO the authority to ensure compliance with the HHS information security program;
- Ensuring that HHS has trained personnel to support compliance with the HHS information security program; and
- Ensuring that the HHS CIO, in coordination with the OPDIV CIOs, reports annually on the effectiveness of the information security program and on remedial actions where required.

2.2.2 Department Leadership

Several leaders in the Department have specific information security responsibilities. The Departmental security leadership includes the following positions:

- HHS CIO;
- OPDIV Heads;
- Deputy Assistant Secretary for Finance;
- Assistant Secretary for Administration and Management (ASAM); and
- Deputy Assistant Secretary for Human Resources.

2.2.2.1 HHS CIO

The HHS CIO is responsible for:

- Reporting annually, in coordination with STAFFDIV and OPDIV Heads, to the Secretary on the effectiveness of the HHS Information Security Program, including progress of remedial actions;
- Developing, promoting, and coordinating the Department-wide information security program activities;
- Appointing the HHS CSO to fulfill the CIO's responsibilities in developing and maintaining an agency-wide security program;
- Defining and establishing the minimum-security control requirements in accordance to data sensitivity and system criticality;
- Preparing any report that may be required of HHS to satisfy reporting requirements on OMB Circular A-130 and FISMA;
- Ensuring the provision of the resources necessary to administer the HHS information security program;
- Providing advice and assistance to the Secretary and other senior management personnel to ensure that information resources are acquired and managed for the agency in accordance with the goals of the Capital Planning and Investment Control (CPIC) process;
- Providing leadership for developing, promulgating, and enforcing agency information resource management policies, standards, and guidelines, and for procedures on data management, system life cycle management, security, telecommunications, IT reviews, and other related areas;
- Establishing, implementing, and enforcing a Department-wide framework to facilitate an incident-response program ensuring proper and timely reporting to the Federal Computer Incident Response Center (FedCIRC); and
- Establishing a Department-wide framework to facilitate the development of Privacy Analysis Worksheets and Privacy Impact Assessment (PIA) Summaries for all Departmental systems, as instructed by OMB.

2.2.2.2 OPDIV Heads

OPDIV Heads are responsible for:

- Providing information security protections commensurate with the risk and magnitude of harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of the following:
    - Information collected or maintained by or on behalf of the OPDIV; and
    - Information systems used or operated by the OPDIV, by a contractor of the OPDIV, or other organization on behalf of the OPDIV.
- Complying with the requirements of FISMA and Department-related policies, procedures, standards, and guidelines, including:
    - Information security requirements promulgated under OMB Circular A-130, Appendix III; and
    - Information security standards and guidelines issued in accordance with NIST.
- Ensuring that information security management processes are integrated with OPDIV strategic and operational planning processes;
- Ensuring that senior OPDIV officials provide information security for the information and information systems that support the operations and assets under their control;
- Designating a senior OPDIV official as the OPDIV CIO and delegating the OPDIV CIO with the authority to ensure compliance with the security requirements imposed on the OPDIV under FISMA;
- Ensuring that the OPDIV has trained personnel sufficiently to assist the OPDIV in complying with the security requirements under FISMA and Departmental policies; and
- Ensuring that the OPDIV CIO, in coordination with other senior OPDIV officials, reports annually to the OPDIV Head on the effectiveness of the OPDIV information security program, including progress of remedial actions.

2.2.2.3 Deputy Assistant Secretary for Finance

The Deputy Assistant Secretary for Finance is responsible for:

- Coordinating the Department's Internal Controls Program, also known as Executive Secretary or ExecSec, to ensure comprehensiveness and to establish responsibility for uniform security-level designations for the financial management systems according to the guidelines of OMB Circular A-127, *Financial Management Systems*.

2.2.2.4 Assistant Secretary for Administration and Management

The ASAM is responsible for:

- Partnering with the HHS CIO and the Department's Office of Security to develop and implement information security-related contract clauses for incorporation in all current and future contracts; and
- Ensuring that contracting officers (CO) enforce the requirements of the information security clause.

2.2.2.5 Deputy Assistant Secretary for Human Resources

The Deputy Assistant Secretary for Human Resources is responsible for:

- Partnering with the HHS CIO and OPDIVs to develop, implement, and oversee personnel security controls for access to sensitive data and for the system administrators who operate critical systems; and
- Ensuring that personnel officers notify the OPDIV Information Systems Security Officer (ISSO), or designated point of contact for physical and logical access controls, of an employee's separation within one business day.

2.2.3 Information Security Leadership

The information security leadership at the Department is responsible for overseeing, developing, and implementing the Department's information security program. The Departmental information security leadership consists of the following roles:

- HHS CSO;
- OPDIV CIOs;
- OPDIV CISOs; and
- OPDIV ISSOs

2.2.3.1 HHS CSO

The HHS CSO is responsible for:

- Managing the Office of Information Technology Security Development and Implementation (OITSDI), which is a subdivision of the Office of Information Resources Management (OIRM);
- Providing leadership in implementing and maintaining an Information Security Program Review for all HHS IT resources and ensuring that reviews are conducted in compliance with established Departmental and external policies, standards, and regulations;
- Monitoring OPDIV systems' security program activities;
- Overseeing the production of the OPDIV Quarterly Information Security Status Report, which provides an assessment of all major programmatic initiatives throughout the OPDIVs;

- Developing and implementing an IT security-performance measurement program to evaluate the effectiveness of technical and nontechnical information security safeguards used to protect the Department's information;
- Managing a Critical Infrastructure Protection Coordinator (CIPC) for creating and maintaining an HHS Critical Infrastructure Protection (CIP) Plan;
- Coordinating requirements within the Office of Security for personnel clearances, position sensitivity, and access to information systems with the appropriate office;
- Ensuring that all HHS-owned Private Branch Exchanges (PBX) are provided system and physical protection;
- Implementing a security-event monitoring program for all systems and networks;
- Disseminating information on recommended safeguards and the potential security threats and concerns of access to Departmental systems; and
- Ensuring PIAs are conducted for electronic information systems and collections and coordinating submission of all Department Privacy Analysis Worksheets and PIA Summaries to OMB.

2.2.3.2 OPDIV CIOs

OPDIV CIOs are responsible for:

- Reporting quarterly to the HHS CIO on the effectiveness of the organization's information security program, including progress of remedial actions;
- Appointing a CISO to fulfill the CIO's responsibilities in maintaining the OPDIV's information security program;
- Managing internal security reviews of the program business cases, alternatives analyses, and other specific investment documents;
- Establishing and implementing policies, procedures, and practices that are consistent with Departmental requirements to assure that systems, programs, and data are secure and protected from unauthorized access that might lead to the alteration, damage, or destruction of automated resources, unintended release of data, and denial of service (DoS);
- Ensuring that all employees and contractors comply with this policy;
- Ensuring the establishment of Incident Response Team(s) (IRT) to participate in the investigation and resolution of incidents in their respective OPDIV;
- Enforcing incident response processes and procedures developed by the Department and the Secure One Communications Center (SOCC);
- Managing an inventory of all major information systems and updating it annually or when a major change has occurred;
- Establishing a framework to facilitate the development of Privacy Analysis Worksheets and PIA Summaries for all OPDIV systems, as instructed by OMB;
- Managing and certifying an inventory of all current and proposed investments that contain an IT component; and
- Ensuring that security education and awareness is mandatory for all personnel using, operating, supervising, or managing computer systems.

2.2.3.3 OPDIV CISOs

OPDIV CISOs are responsible for:

- Leading OPDIV information security programs and promoting proper information security practices;
- Supporting the HHS CSO's implementation of the HHS Information Security Program;
- Providing information about the OPDIV information security policies to management and throughout to the organization;
- Providing advice and assistance to other organizational personnel concerning the security of sensitive data and the security of critical data processing capabilities;
- Advising the CIO about security breaches in accordance with the security breach reporting procedures developed and implemented by the OPDIV;
- Disseminating information on recommended safeguards and the potential security threats and concerns of access to OPDIV systems;
- Conducting security education and awareness training needs assessments to determine appropriate training resources and coordinate training activities for target populations;
- Assisting system owners in establishing and implementing the appropriate security safeguards required to protect computer hardware, software, and data from improper use or abuse;
- Working with the CIPC to identify critical IT infrastructures and develop plans for protecting them; and
- Coordinating requirements for personnel clearances, position sensitivity, and access to information systems with the appropriate office.

2.2.3.4 OPDIV ISSOs

OPDIV ISSOs are responsible for:

- Leveraging the OPDIV security awareness program, that shall include initial and annual refresher training, to communicate the security policies effectively to users at all levels;
- Notifying the OPDIV CISO of computer-security incidents (or suspected incidents);
- Ensuring that information security notices and advisories are distributed to appropriate OPDIV personnel and that vendor-issued security patches are expeditiously installed;
- Serving as an OPDIV focal point for incident reporting and subsequent resolution;
- Assisting the CISO in reviewing contracts for systems under his/her control to ensure that information security is appropriately addressed in contract language;
- Assisting the CISO in ensuring that system weaknesses are captured in the Plan of Action and Milestone (POA&M);

- Re-enforcing the concept of separation of duties by ensuring that single individuals do not have control of the entirety of a critical process;
- Tracking all security education and awareness conducted for personnel and contractors;
- Assisting the CISO in enforcing proper backup procedures for all system and network information;
- Assisting the CISO in enforcing logical access controls that provide protection from unauthorized access, alteration, loss, disclosure, and availability of information;
- Enforcing account lockout controls that limit the number of consecutive failed log on attempts against a given system;
- Assisting the CISO in enforcing limits for the amount of time a session may be inactive before that session is timed out;
- Ensuring that security-event monitoring technologies are used for all systems and networks;
- Assisting the CISO in coordinating with Human Resource management to develop reporting procedures regarding personnel departures from the Department;
- Assisting the CISO in enforcing all incoming and outgoing connections from Departmental networks to the Internet, intranet, and extranets are made through a firewall;
- Enforcing a malicious code protection program designed to minimize the risk of introducing malicious code into information systems and networks; and
- Analyzing audit logs carefully and frequently and monitoring the types of assistance users request.

2.2.3.5 CIO Council

The CIO Council is responsible for:

- Deliberating and approving technical recommendations from the CISO Working Group.

2.2.3.6 CISO Working Group

The CISO Working Group is responsible for:

- Working together to review differences of technical opinion, and passing recommendations up to the CIO Council.

2.2.4 Information Security Roles

Within the HHS Information Security Program, persons in other roles have responsibilities related to maintaining the information security posture of the Department. These roles include:

- Designated Approving Authority (DAA);
- Certification Authority (CA);

- Program executive;
- Critical Infrastructure Protection Coordinator (CIPC);
- Contingency Planning Coordinator;
- System owners;
- Data owner;
- System/Network administrators;
- Contracting officers (CO);
- Personnel officers;
- Supervisors; and
- Users and employees.

2.2.4.1 Designated Approving Authority

The DAA is the CIO, or other person designated by the CIO, and has the following responsibilities for systems and networks under his/her authority:

- Determining, through the security accreditation process, whether the level of risk remaining, once security procedures and controls have been implemented, provides protection commensurate with a system's sensitivity;
- Determining, based on the analysis provided by the CA or his or her designee, whether to accept a risk or to implement countermeasures;
- Being accountable for the residual risks accepted;
- Making the final decision on the type of accreditation and signing the document prepared by the CA or his or her designee to document the decision; and
- Ensuring that sensitive data is protected from unauthorized access in all forms at rest or in transit.

2.2.4.2 Certification Authority

The CA has the following responsibilities for systems and networks under his/her authority:

- Ensuring the certification of all the Department's systems and networks;
- Conducting the certification and accreditation (C&A) process in accordance with NIST or the National Information Assurance Certification and Accreditation Process (NIACAP); and
- Reviewing security documentation provided by system owners and the results of the Security Testing and Evaluation (ST&E) and documenting their recommendation for acceptance or rejection of risk and accreditation or non-accreditation.

2.2.4.3 Program Executives

Program executives are responsible for:

- Ensuring that systems and data that are critical to the program's mission receive adequate protection;

- Determining, in coordination with the business owner and system owner, appropriate security controls and identifying resources to implement those controls;
- Coordinating system and data security requirements with IT security personnel by adequately delegating system-level security requirements; and
- Accepting reasonable risks, based on recommendations by their HHS CSO or OPDIV CISO or ISSO.

2.2.4.4 Critical Infrastructure Protection Coordinator

The CIPC is responsible for:

- Creating and maintaining a CIP Plan;
- Identifying critical IT infrastructures and developing plans for protecting those infrastructures; and
- Creating and maintaining a Department-wide inventory of all critical IT infrastructures and ranking each element of those infrastructures by level of criticality.

2.2.4.5 Contingency Planning Coordinator

The Contingency Planning Coordinator is responsible for:

- Approving the contingency strategy and designating appropriate teams to implement the strategy;
- Ensuring that each team is trained and ready to deploy in the event of a disruptive situation requiring contingency plan activation; and
- Ensuring that recovery personnel are assigned to each team to respond to the event, recover capabilities, and return the system to normal operations.

2.2.4.6 System Owners

System owners are responsible for:

- Being liable for the operation of a system(s) in support of the program mission;
- Processing systems at facilities and Information Technology Utilities (ITU) that are certified at a level of security equal to or higher than the security level designated for their system;
- Ensuring that information and system categorization has been established for their systems and data in accordance with FIPS Publication 199;
- Determining, in coordination with the program executive and data owner, appropriate security controls and identifying resources to implement those controls;
- Consulting with the Department or OPDIV CIO to establish consistent methodologies for determining IT security costs for systems;

- Ensuring that for each information system, security is planned for, documented, and integrated into the system life cycle (SLC) from the information system's initiation phase to the system's disposal phase;
- Conducting PIAs in coordination with their respective CIO or CISO on their systems used to collect information on individuals or when the Department develops, acquires, or buys new systems, to handle collecting information in identifiable form;
- Conducting assessments of the risk and magnitude of the harm that would result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the Department's critical operations, at least annually;
- Reviewing the security controls for their systems and networks when significant modifications are made to the system and network, and/or at least every three years;
- Ensuring that system weaknesses are captured in the POA&M;
- Ensuring that sensitivity and criticality levels have been established for their systems and data in accordance with NIST standards and guidelines;
- Developing System Security Plans (SSP) for their systems and networks;
- Obtaining written authorization from management (e.g., DAA, Departmental CSO or OPDIV CISO) prior to connecting with other systems and/or sharing sensitive data/information;
- Developing system rules of behavior for systems under their responsibility;
- Conducting annual reviews and validations of system users' accounts to ensure the continued need for access to a system;
- Enforcing the concept of separation of duties by ensuring that single individuals do not have control of the entirety of a critical process;
- Ensuring that special physical security or environmental security requirements are implemented for facilities and equipment used for processing, transmitting, or storing sensitive information based on the level of risk; and
- Ensuring the development, execution, and activation of a system-to-system interconnection implementation plan for each instance of a system-to-system interconnection.

2.2.4.7 Data Owners

Data owners are responsible for:

- Gathering, processing, storing, or transmitting Departmental data in support of the program's mission; and
- Ensuring that system owners are aware of the sensitivity of data to be handled and ensuring that data is not processed on a system with security controls that are not commensurate with the sensitivity of the data.

2.2.4.8 System/Network Administrators

System/Network administrators are responsible for:

- Ensuring that appropriate security requirements are implemented and enforced for all Departmental systems or networks;
- Implementing proper system backups, patching security vulnerabilities, and accurately reporting security incidences;
- Utilizing his/her “root” or “administrative” access rights to a computer based on need to know;
- Ensuring that the information security posture of the network is maintained during all network maintenance, monitoring activities, installations or upgrades, and throughout day-to-day operations;
- Implementing appropriate technical security on their information systems; and
- Resolving an incident situation by isolating the intrusion and protecting other systems connected to the network until assurance can be made that the problem has been adequately resolved and will not recur.

2.2.4.9 Contracting Officers

COs are responsible for:

- Ensuring that all IT acquisitions include the Department’s security considerations in each contract;
- Ensuring that the appropriate security contracting language is incorporated in each contract; and
- Maintaining the integrity and quality of the proposal evaluation, negotiation, and source selection processes while ensuring that all terms and conditions of the contract are met.

2.2.4.10 Personnel Officers

Personnel officers are responsible for:

- Notifying the OPDIV ISSOs within one business day when OPDIV personnel are separated from the Department; if the ISSO is not available, the personnel officer should contact the appropriate OPDIV CISO.

2.2.4.11 Supervisors

Supervisors are responsible for:

- Ensuring compliance with information security policies by all personnel under their direction and providing the personnel, financial, and physical resources required to protect information resources appropriately;
- Ensuring that their direct reports complete all required IT security training within the mandated time frame;
- Notifying the appropriate OPDIV ISSO immediately of the unfriendly departure or separation of a Department or contractor; if the ISSO is not available, then they should contact the appropriate OPDIV CISO immediately; and

- Pursuing disciplinary or adverse actions against personnel and contractors who violate the *HHS Information Security Program Policy, HHS Information Security Program Rules of Behavior,* and system-specific rules of behavior.

2.2.4.12 Users and Employees

The Department's users and employees are responsible for:

- Complying with the Department's policies, standards, and procedures;
- Being aware they are *not* acting in an official capacity when using Departmental IT resources for non-governmental purposes;
- Familiarizing themselves with any special requirements for accessing, protecting, and using data, including Privacy Act requirements, copyright requirements, and procurement-sensitive data;
- Reporting any suspected or actual computer incidents immediately to the OPDIV IRT;
- Seeking guidance from their supervisors when in doubt about implementing this policy document;
- Ensuring that all media containing Departmental data is appropriately marked and labeled to indicate the sensitivity of the data;
- Refraining from loading unapproved software on Departmental systems or networks;
- Ensuring that sensitive data is not stored on laptop computers or other portable devices unless the data is secured using encryption standards that are commensurate with the sensitive level of the data;
- Reading, acknowledging, signing, and complying with the *HHS Information Security Program Rules of Behavior* and OPDIV- and system-specific rules of behavior before gaining access to the Department's systems and networks;
- Implementing specified security safeguards to prevent fraud, waste, or abuse of the systems, networks, and data they are authorized to use;
- Conforming to security policies and procedures that minimize the risk to the Department's systems, networks, and data from malicious software and intrusions;
- Agreeing not to disable, remove, install with intent to bypass, or otherwise alter security settings or administrative settings designed to protect Departmental IT resources; and
- Ensuring that adequate protection is maintained on their workstation, including not sharing passwords with any other person and logging out, locking, or enabling a password-protected screen saver before leaving their workstation.

2.2.5 Department Security Council

2.2.5.1 Information Technology Investment Review Board

The Information Technology Investment Review Board (ITIRB) is responsible for:

- Selecting, evaluating, and controlling IT investments; and
- Ensuring IT investments are appropriately addressing IT security consideration in a manner commensurate with risk.

3. Management Policies

3.1 Capital Planning and Investment

Integrate and explicitly identify funding for information security technologies and programs into IT investment and budgeting plans. Establish consistent methodologies for determining information security costs for all Departmental systems and networks. Ensure that any Departmental system that is reported to FISMA must be mapped to an exhibit 300 and/or exhibit 53. This policy should be implemented in coordination with the HHS-IRM-2000-0001, *HHS IRM Policy for Capital Planning and Investment Control*, January 8, 2001.

3.2 Contractors and Outsourced Operations

Implement appropriate safeguards to protect Departmental systems and networks from unauthorized access throughout all phases of a contract. Review contracts to ensure that information security is appropriately addressed in the contracting language.

3.3 Security Performance Measures and Metrics

Develop and implement an information security performance measurement program to evaluate the effectiveness of technical and nontechnical information security safeguards, support mandatory data collections required by Congress, OMB, and the Office of Inspector General (OIG), and enable the creation, analysis, and reporting of information security performance measures selected by the Department. The program shall be linked to the Department's strategic plan and include measures of implementation, efficiency, effectiveness, and impact. Report all measures to the Secretary quarterly.

3.4 Critical Infrastructure Protection Support

Establish and implement a CIP program to comply with the Homeland Security Presidential Directive/HSPD-7, *Critical Infrastructure Identification, Prioritization, and Protection*, December 17, 2003, and develop and document a CIP Plan that identifies Departmental critical infrastructures and plans to minimize vulnerabilities.

3.5 System Life Cycle

Integrate security into the SLC for all Departmental systems from inception to the disposal phases of the system through adequate and effective management, personnel, operational, and technical control mechanisms.

3.6 Change Management Control

Establish, implement, and enforce change management and configuration management controls on all Departmental systems and networks that process, store, or communicate sensitive information, to include the preparation of configuration control plans for all Departmental systems and networks.

3.7 Risk Management

Establish and implement a risk-management program, responsibilities, and processes for all Departmental personnel, systems, networks, data, and facilities that house them.

3.7.1 Security Program Review

Conduct independent security program reviews on all Departmental information security programs to determine the program's effectiveness, at least annually.

3.7.2 Security Control Review

Review all security controls on all Departmental systems, networks, and interconnected systems to ensure that adequate security controls are implemented to prevent unauthorized access, use, disclosure, disruption, modification, or destruction of information, at least annually.

3.7.3 Risk Assessments

Conduct assessments of the risk and magnitude of the harm that would result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems and networks that support Departmental operations when significant modifications are made and/or at least every three years.

3.7.4 System Interconnectivity/Information Sharing

Obtain written authorization from management (e.g., DAA) prior to connecting with other systems and/or sharing sensitive data/information.

3.8 Privacy Impact Assessments

Conduct PIAs on all Departmental information systems as instructed by OMB Memorandum M-03-22 that includes, but is not limited to, the collection of new information in identifiable form (IIF) or when the Department develops, acquires, and/or buys new information systems to handle collections of IIF. PIAs are also required when significant changes are made to these systems. Maintain both soft and

signed hard copies of all PIAs and submit electronically both parts of the PIA (Analysis Worksheets and PIA Summary) to the HHS CSO. This policy shall be implemented as required by Section 208(b) of the *E-Government Act of 2002* (Public Law 107-347, U.S.C. Title 44, Chapter 36) and consistent with the intent of OMB Memorandum (M)-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002.*

3.9 Self-Assessments

Conduct self-assessments on all Departmental systems and networks at least annually in accordance with NIST SP 800-26, *Security Self-Assessment Guide for Information Technology Systems*. Maintain and submit all NIST Self-Assessments to the HHS CSO.

3.10 Plan of Action and Milestones

Capture all information security program and system weaknesses that require mitigation in the POA&M in accordance with the standards and guidelines set forth by OMB and the HHS CSO.

3.11 System Inventory

Develop and maintain an inventory of all Departmental systems and networks and update annually or when significant changes occur to the system. Maintain and submit all system inventories to the appropriate Departmental Enterprise Architect. The Enterprise Architect will be responsible for reporting any changes or updates to the HHS CSO. This policy shall be implemented as required by the Clinger-Cohen Act, Division E, Section 5402, and as required by FISMA, Section 305.

3.12 System Categorization

Establish and document all Departmental systems, networks, and data categorizations in accordance with FIPS 199, *Standards for Security Categorization of Federal Information and Information*, February 2004.

3.13 System Security Plans

Develop and document SSPs for all Departmental systems and networks in accordance with NIST SP 800-18, *Guide for Developing Security Plans for Information Technology Systems.* Update SSPs at least once every three years or when significant changes occur to the system.

3.14 Authorize Processing (Certification and Accreditation)

Ensure that all Departmental systems and networks are formally certified through a comprehensive evaluation of the technical and nontechnical security features. Any significant changes occurring to Departmental systems, networks, or to its physical environment, users, etc., require a review of the impact on the security of the information processed and shall require re-accreditation. All systems will be re-accredited every three years at a minimum or when a major change occurs. Maintain and submit all accreditation letters to the HHS CSO.

3.15 Policy Waiver

Obtain written authorization (form located in Appendix F) from the OPDIV CISO if compliance with the *HHS Information Security Program Policy* is not feasible or technically possible, or if an OPDIV needs to deviate from a policy to support its mission or business function. The OPDIV will have 60 days to file the waiver or become compliant with the policy in question. All policy waivers must be recorded and maintained for inspection by the HHS CSO.

4. Operational Policies

4.1 Personnel Security

4.1.1 Background Investigations

Ensure that all Departmental information security employees and contractor personnel are designated with position-sensitivity levels that are commensurate with the responsibilities and risks associated with the position. Require suitability background investigations to be completed and favorably adjudicated for personnel assigned to these positions prior to allowing access to sensitive Departmental systems and networks.

Perform reinvestigations in accordance with the guidance provided in the *HHS Information Technology Personnel Security Guide.*

4.1.2 Rules of Behavior

Develop system rules of behavior for all Departmental systems and networks that include specific security rules for each system. Require all Department system users to read, acknowledge, and comply with their roles and responsibilities and security rules of each system. Require all users to sign a rules of behavior agreement prior to being granted full access to all Departmental systems and networks. Digital signatures may be employed; however, if the technology is not available, then the individual's original signature should be obtained to acknowledge the receipt of the appropriate rules of behavior.

4.1.3 Disciplinary Action

Enforce disciplinary or adverse actions against Departmental employees or contractors who violate the *HHS Information Security Program Policy*, *HHS Information Security Program Rules of Behavior*, and system-specific rules of behavior.

4.1.4 Acceptable Use

Limit personal use of all Departmental IT resources, which include computers, telecommunications equipment, software, and other data/information services (e.g., e-mail and Internet) provided on the Departmental networks. Personal use of IT resources shall not compromise the security posture of the Department's IT resources. This policy should be implemented in coordination with the HHS-IRM-2004-0001, the *HHS IRM Policy for Personal Use Of Information Technology Resources*, November 23, 2004.

4.1.5 Separation of Duties

Ensure that responsibilities with a security impact are shared among multiple staff by enforcing the concept of separation of duties, which requires that individuals do not have control of the entirety of a critical process.

Ensure that job descriptions accurately reflect assigned duties and responsibilities that support separation of duty.

4.1.6 Least Privilege

Ensure that all Departmental systems operate in such a way that they run with the least amount of system privilege needed to perform a specific function and that system access be granted on a need to know basis.

Enforce compliance with executive, legislative, and technical requirements to ensure that only appropriate personnel are granted access to sensitive information or system privileges.

4.1.7 Security Education and Awareness

Ensure new Departmental users receive initial security education and awareness training before being granted permanent access to Departmental systems and networks. Access to administrative systems, such as electronic or online training, can be granted for new employees on a temporary basis. All Departmental users shall receive annual (refresher) training in security education and awareness.

Provide specialized security education and awareness training for all security positions and roles that is commensurate with the individual's duties and responsibilities.

4.1.8 Personnel Separation

Upon Departmental employee or contractor termination, or other departure, ensure all access and privileges to Departmental systems, networks, and facilities are immediately revoked.

4.2 Physical Security

4.2.1 Physical Access

Limit access to rooms, work areas/spaces, and facilities that contain Departmental systems, networks, and data to authorized personnel. Controls shall be in place for deterring, detecting, monitoring, restricting, and regulating access to sensitive areas at all times. Controls must be commensurate with the level of risk and must be sufficient to safeguard these IT resources against possible loss, theft,

destruction, accidental damage, hazardous conditions, fire, malicious actions, and natural disasters.

4.2.2 Physical Security

Ensure that rooms, work areas/spaces, and facilities that contain Departmental IT resources that process, transmit, or store sensitive or privacy information implement physical protection measures that are commensurate with the level of risk.

4.2.3 Visitor Policy

Restrict and control visitor access at all times to rooms, work areas/spaces, and facilities that contain Departmental IT resources. Records that contain visitor access information shall be maintained.

4.3 Environmental Security

Ensure that all Departmental systems and networks are located in areas not in danger of water damage due to leakage from building plumbing lines, shut-off valves, and other similar equipment to support meeting federal and local building codes. Implement procedures to address infrastructure emergencies and provide access to the Department.

4.3.1 Fire Prevention

Install and ensure operability of fire suppression devices, such as fire extinguishers and sprinkler systems, and detection devices, such as smoke and water detectors, in all areas where Departmental critical systems are maintained (this includes server rooms, tape libraries, and data centers) to meet federal and local building codes.

4.3.2 Supporting Utilities

Install and ensure operability of air control devices, such as air-conditioners and humidity controls, in all areas where Departmental critical systems are maintained (this includes server rooms, tape libraries, and data centers) to meet federal and local building codes.

4.4 Media Control

4.4.1 Media Protection

Protect all Departmental electronic media (e.g., disk drives, diskettes, internal and external hard drives, and portable devices), including backup media, removable media, and media containing sensitive information from unauthorized access.

4.4.2 Media Marking

Ensure that all media containing Departmental data is appropriately marked and labeled to indicate the sensitivity level of the data.

4.4.3 Sanitization and Disposal of Information

Ensure that sanitization and disposal methods are commensurate with the sensitivity and criticality of Departmental data residing on storage devices, equipment, and hard copy.

4.4.4 Input/Output Controls

Implement physical, administrative, and technical controls to prevent unauthorized entry into office suites, operations, data storage, library, and other restricted areas. These controls shall restrict the unauthorized removal of media.

4.5 Data Integrity

Ensure that the appropriate Departmental systems and networks are equipped with data integrity and validation controls to provide assurance that Departmental information has not been altered.

4.5.1 Documentation

Ensure that all Departmental system and network documentation is developed, readily available to appropriate personnel, secured, and up to date for routine security audits, tests, and unexpected events, such as system disruptions or outages.

4.6 Communications Security

4.6.1 Voice Communications

Ensure that all Department-owned voice communication networks provide adequate security controls at the system and environmental levels.

4.6.2 Data Communications

Ensure that sensitive data is protected from unauthorized access during transmission.

4.6.3 Video Teleconferencing

Implement adequate controls to ensure that only authorized individuals attend a specific video teleconference. Ensure that appropriate transmission protections are in place commensurate with the highest sensitivity of information to be discussed over the video teleconference.

4.6.4 Audio Teleconferencing

Implement adequate controls to ensure that only authorized individuals attend a specific audio teleconference. Ensure that appropriate transmission protections are in place commensurate with the highest sensitivity of information to be discussed over the audio teleconference.

4.6.5 Webcast

Implement adequate controls to ensure that only authorized individuals attend a specific Webcast and are able to participate in transmitting or receiving voice, data, and graphics over the World Wide Web. Ensure that appropriate transmission protections are in place commensurate with the highest sensitivity of information (voice, data, or graphics) to be transmitted or received over the Webcast.

4.6.6 Voice-Over Internet Protocol

Ensure that the use of voice-over Internet Protocol (IP) equipment to transmit or discuss sensitive data is protected with encryption standards that are commensurate with the sensitivity level of the data.

4.6.7 Facsimile

Ensure that appropriate technical controls are implemented and enforced for facsimile technology and systems that can be used to transmit and receive sensitive information. Facsimile communications that require secure communications shall use systems configured to use encryption standards that are commensurate with the sensitivity level of the data.

4.7 Wireless Communications Security

4.7.1 Wireless Local Area Network (LAN)

Ensure that the appropriate Departmental CIO approves the overall wireless plan for his/her respective organization. Wireless networks shall not be connected to wired Departmental networks except through appropriate controls (e.g., Virtual Private Network (VPN) port). Wireless LANs may not be used to transmit, process, or store sensitive information unless protected with encryption standards that are commensurate with the sensitivity level of the data.

4.7.2 Multifunctional Wireless Devices

Ensure that sensitive data is not transmitted using wireless devices unless secured with encryption standards that are commensurate with the sensitivity level of the data.

4.8 Equipment Security

4.8.1 Workstations

Ensure that security controls that are commensurate with the sensitivity level of the data are maintained on all Departmental workstations.

4.8.2 Laptops and Other Portable Computing Devices

Ensure that the storage and transmission of Departmental sensitive data on laptop and portable computing devices are protected with encryption standards that are commensurate with the sensitivity level of the data.

4.8.3 Personally Owned Equipment and Software

Control the use of personally owned or non-Departmental equipment and software to process, access, or store sensitive data. Personally owned or non-Departmental equipment and software includes, but is not limited to, personal computers and related equipment and software, Internet service providers, personal e-mail providers (e.g., Yahoo, Hotmail), personal library resources, handheld and Personal

Digital Assistant (PDA) devices, facsimile machines, and photocopiers. Such personally owned equipment and software shall not be used to process, access, or store sensitive information, or be connected to Departmental systems or networks without the written authorization from the appropriate Departmental CISO.

Require the use of encryption capabilities conforming to FIPS Publication 140-2, *Security Requirements for Cryptographic Modules,* when transmitting and storing sensitive information on personally owned equipment. Remote connection for telecommuting Departmental employees and contractors shall be executed in accordance with the Departmental policy for remote access and dial-in.

4.8.4 Hardware Security

Ensure that hardware products provide dependable, cost-effective security controls and features and preserve the integrity of the security features provided through the system software.

4.8.5 Software Security

Implement software security features that are commensurate with the sensitivity level of the data. The security controls selected must protect information resources from unauthorized access or modification.

4.8.6 Hardware/Software Maintenance

Ensure all Departmental hardware and software is tested, documented, and approved prior to promotion to production. Ensure that only authorized personnel conduct maintenance on all Departmental hardware and software.

4.9 Contingency Planning

Ensure contingency plans for all Departmental systems, networks, data, business process, and facilities are coordinated and aligned together and tested annually. Refer to the *HHS Contingency Planning for Information Security Guide* for implementation best practices.

4.9.1 Security Incident and Violation Handling

Establish and maintain an incident response capability to include preparation, identification, containment, eradication, recovery, and follow-up capabilities to ensure effective recovery from incidents. IRTs shall document and report all security incidents to the HHS SOCC, which will provide updates to the HHS CSO. Ensure that evidence of computer crimes is properly preserved. This policy should be implemented in coordination with the HHS-IRM-2000-0006, *HHS IRM Policy for Establishing an Incident Response Capability*, January 8, 2001.

4.9.2 IT Disaster Recovery

Identify, prioritize, and document disaster recovery (DR) planning requirements for all critical Departmental systems, networks, data, and facilities based on requirements set forth in FISMA; OMB Circular A-130, Appendix III; Federal Preparedness Circular (FPC) 65, *Federal Executive Branch Continuity of Operations;* Presidential Decision Directive (PDD) 67, *Enduring Constitutional Government and Continuity of Government Operations;* Federal Emergency Management Agency (FEMA), Federal Response Plan (FRP); and NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems*. The DR plan and procedures shall be tested annually or as significant changes are made. Refer to the disaster recovery section of the *HHS Contingency Planning for Information Security Guide* for implementation best practices.

4.9.3 Backup Data

Implement and enforce proper backup procedures for all system and network information based on the sensitivity and criticality of the data.

4.9.4 Store Backup Data

Ensure that backup data is stored a safe distance from the primary system, does not share the same environmental conditions as the primary system, and is not at risk for the same disruptions as the primary system.

5. Technical Policies

5.1 Identification and Authentication

Implement and enforce user Identification and Authentication (I&A) techniques for all Departmental systems and networks in a manner commensurate with the risk and sensitivity of the system, network, and data.

5.1.1 Identification

Establish individual accountability for all Departmental systems and networks using user identifications (UserID). UserIDs shall be unique to each authorized user.

5.1.2 Password

Implement and enforce logical password controls for all Departmental systems and networks. Require passwords to remain confidential and to be used for all Departmental systems and networks where more than “read” authority is available to the user.

5.2 Access Control

Implement logical access controls that provide protection from unauthorized access, alteration, loss, disclosure, and availability of information. This policy should be implemented in coordination with the HHS-IRM-2000-0007, *HHS IRM Policy for the Prevention, Detection, Removal and Reporting Of Malicious Software*, January 8, 2001.

5.2.1 Review and Validation of System User Accounts

Conduct annual reviews and validations of system users’ accounts to ensure the continued need for access to a system.

5.2.2 Automatic Account Lockout

Implement and enforce account lockout controls that limit the number of consecutive failed log-on attempts against all Departmental systems and networks.

5.2.3 Automatic Session Timeout

Establish and implement limits of time that a session is allowed to remain idle before it is automatically timed out.

5.2.4 Warning Banner

Ensure that all Departmental systems and networks display Department-approved sign-on warning banners at all system access points.

5.3 Audit Trails

Ensure all Departmental systems and networks generate audit logs that show addition, modification, and/or deletion of information. Ensure that audit logs are protected from unauthorized modification, access, or destruction and are recorded, retained, and regularly analyzed to identify unauthorized activity.

5.4 Network Security

5.4.1 Remote Access and Dial-In

Implement and enforce remote access and dial-in security controls to provide protection for information that is stored, accessed, transmitted, and received across public or private networks. This policy should be implemented in coordination with the HHS-IRM-2000-0005, *HHS IRM Policy for IT Security for Remote Access*, January 8, 2001.

5.4.2 Network Security Monitoring

Implement a security event-monitoring program for all Departmental systems and networks.

5.4.3 Firewall

Ensure that all incoming and outgoing connections from Departmental systems and networks to the Internet, intranets, and extranets are made through a firewall.

5.4.4 Internet Security

Ensure that the Department's connectivity to the Internet is within a framework of effective technical security controls using firewalls and gateways that provide external network access via Internet Service Providers (ISP) and other public or designated external entities.

5.4.5 E-Mail Security

Protect e-mail services against malicious code attacks and ensure that e-mail services are not used to relay unauthorized messages.

5.4.6 Personal E-Mail Accounts

Prohibit Departmental employees and contractors from transmitting sensitive information using any personal e-mail accounts (e.g., Hotmail, Yahoo, MSN).

5.4.7 Security Testing and Vulnerability Assessment

Ensure that all Departmental systems and networks containing sensitive or mission critical information undergo vulnerability scanning and/or penetration testing to identify security threats at least annually or when significant changes are made to the system or network.

5.5 Cryptography

Ensure that all information requiring protection from unauthorized disclosure is encrypted during transmission using current NIST encryption standards and Department-approved encryption products. Departmental employees and contractors shall not transmit such information without using cryptographic protections.

5.6 Malicious Code Protection

Implement and enforce a malicious code protection program designed to minimize the risk of introducing malicious code (e.g., viruses, worms, Trojan horses) into all Departmental systems and networks. This policy should be implemented in coordination with the HHS-IRM-2000-0007, *HHS IRM Policy for the Prevention, Detection, Removal and Reporting Of Malicious Software*, January 8, 2001.

5.7 Product Assurance

Ensure that the appropriate implementation of evaluated and approved technology products is required for all Departmental systems used to store, process, display, or transmit sensitive or privacy information.

5.8 System-to-System Interconnection

Implement a plan to establish, maintain, and terminate interconnections among Departmental systems and networks that are owned and operated by different organizations, including organizations within another federal agency.

5.9 Peer-to-Peer Communications

Ensure the use of secure instant messaging and peer-to-peer file sharing software on all Departmental systems and networks, where appropriate.

5.10 Patch Management

Implement security patches to all Departmental systems and networks in a manner that ensures maximum protection against security vulnerabilities and minimum impact on Departmental business operations. Patch management must contain a systematic process of identifying, prioritizing, acquiring, implementing, testing, and validating security patches necessary for each system or network. A risk-based decision must be documented if security patches are not applied to a system or network. The OPDIV CISO must approve all patch management policies.

Appendix A: Document Feedback

This form is for reviewer suggested corrections, revisions, or updates to improve the usefulness of the document for possible inclusion in future versions. Please forward recommended changes and comments to the U.S. Department of Health and Human Services (HHS), Office of Information Resources Management (OIRM).

By E-mail: SecureOne.HHS@hhs.gov
Subject Line: Policy Feedback
By Phone: (202) 690-6162

Document Title:
>
Section Number:
>
Category of Comment:

A	Administrative. Administrative comments correct what appear to be inconsistencies between sections, typographical errors, or grammatical errors.
S	Substantive. Substantive comments correct sections in the publication that appear to be or are potentially incorrect, incomplete, misleading, or confusing.
C	Critical. Critical comments will cause non-concurrence with the publication if concerns are not satisfactorily resolved.
M	Major. Major comments are significant concerns that may result in a non-concurrence of the entire document if not satisfactorily resolved. This category may be used with a general statement of concern with a subject area, thrust of the document, etc., followed by detailed comments on specific entries in the publication which, taken together, constitute the concern.

Category	**Comment**

Name of Submitting Operating Division (OPDIV):
>
Your Name and Title:
>
Telephone:
>
E-mail:
>
Note: Use an additional blank sheet if needed.

Appendix B: References

Executive Orders (E.O.)

E.O. 10450, *Security Requirements for Government Employment*, April 27, 1953.

E.O. 12333, *United States Intelligence Activities*, December 4, 1981.

E.O. 12958, *Classified National Security Information*, April 17, 1995.

E.O. 13010, *Critical Infrastructure Protection*, July 15, 1996.

E.O. 13011, *Federal Information Technology*, July 16, 1996.

E.O. 13103, *Computer Software Piracy*, September 30, 1998.

E.O. 13228, *Establishing the Office of Homeland Security and the Homeland Security Council*, October 10, 2001.

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

Federal Preparedness Circulars (FPC)

FPC 65, *Federal Executive Branch Continuity of Operations,* July 26, 1999.

Presidential Decision Directives (PDD)

PDD 67, *Enduring Constitutional Government and Continuity of Government Operations*, October 21, 1998.

Homeland Security Presidential Directive/HSPD-7, *Critical Infrastructure Identification, Prioritization, and Protection*, December 17, 2003.

Public Laws

Public Law 83-703, *Atomic Energy Act of 1954*, August 30, 1954.

Public Law 93-579, *Privacy Act of 1974*, December 31, 1974.

Public Law 97-255*, Federal Manager's Financial Integrity Act of 1982* [H.R. 1526], September 8, 1982.

Public Law 99-474, *Computer Fraud and Abuse Act of 1986*.

Public Law 103-62, *Government Performance and Results Act of 1993*, August 3, 1993.

Public Law 104-106, Division E, *Clinger-Cohen Act of 1996 (formerly Information Technology Management Reform Act)*, February 10, 1996.

Public Law 104-191, *Health Insurance Portability and Accountability Act (HIPAA) of 1996*, August 21, 1996.

Public Law 107-347 [H.R. 2458], *The E-Government Act, Title II — Federal Management and Promote of Electronic Government Services,* and *Title III — Information Security Federal Information Security Management Act (FISMA)* December 17, 2002.

Office of Management and Budget (OMB)

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

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

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

OMB Circular A-130, *Management of Federal Information Resources,* Appendix III, *Security of Federal Automated Information Resources*, November 28, 2000.

OMB Memoranda (M)

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

OMB M-00-13, *Privacy Policies and Data Collection on Federal Web Sites*, June 22, 2000.

OMB M-02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*, October 17, 2001.

OMB 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.

OMB M-03-09, *Reporting Instructions for the Government Information Security Reform Act and Updated Guidance on Security Plans of Action and Milestones*, August 6, 2003.

OMB M-03-10, *Planning for the President's Fiscal Year 2005 Budget Request,* April 25, 2003.

OMB M-03-18, *Implementation Guidance for the E-Government Act of 2002*, August 1, 2003.

OMB M-03-19, *Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting*, August 6, 2003.

OMB M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, September 30, 2003.

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

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

National Archives and Records Administration (NARA)

36 Code of Federal Regulations (CFR) Chapter XII, Subchapter B, *Records Management*, Part 1234, *Electronic Records Management*, (last amended on May 16, 2001).

National Computer Security Center (NCSC)

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

National Institute of Standards and Technology (NIST)

Federal Information Processing Standards (FIPS) Publications

FIPS Publication 140-2, *Security Requirements for Cryptographic Modules*, June 2001.

FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.

Special Publications (SP)

NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook,* October 1995.

NIST SP 800-13, *Telecommunications Security Guidelines for Telecommunications Management Network,* October 1995.

NIST SP 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, September 1996.

NIST SP 800-15, *Minimum Interoperability Specification for PKI Components (MISPC) Version 1,* January 1998.

NIST SP 800-16, *Information Technology Security Training Requirements: A Role- And Performance-Based Model (supersedes NIST SP 500-172),* April 1998.

NIST SP 800-17, *Modes of Operation Validation System (MOVS): Requirements and Procedures,* February 1998.

NIST SP 800-18, *Guide for Developing Security Plans for Information Technology Systems*, December 1998.

NIST SP 800-19, *Mobile Agent Security*, October 1999.

NIST SP 800-20, *Modes of Operation Validation System for the Triple Data Encryption Algorithm (TMOVS): Requirements and Procedures,* April 2000.

NIST SP 800-21, *Guideline for Implementing Cryptography in the Federal Government*, November 1999.

NIST SP 800-22, *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications,* October 2000.

NIST SP 800-23, *Guideline to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products,* August 2000.

NIST SP 800-24, *PBX Vulnerability Analysis: Finding Holes in Your PBX Before Someone Else Does,* August 2000.

NIST SP 800-25, *Federal Agency Use of Public Key Technology for Digital Signatures and Authentication*, October 2000.

NIST SP 800-26, *Security Self-Assessment Guide for Information Technology Systems*, November 2001.

NIST SP 800-27, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security)*, June 2001.

NIST SP 800-28, *Guidelines on Active Content and Mobile Code,* October 2001.

NIST SP 800-29, *A Comparison of the Security Requirements for Cryptographic Modules in FIPS 140-1 and FIPS 140-2,* June 2001.

NIST SP 800-30, *Risk Management Guide for Information Technology Systems*, January 2002.

NIST SP 800-31, *Intrusion Detection Systems (IDS)*, November 2001.

NIST SP 800-32, *Introduction to Public Key Technology and the Federal PKI Infrastructure*, February 2001.

NIST SP 800-33, *Underlying Technical Models for Information Technology Security*, December 2001.

NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems*, June 2002.

NIST SP 800-35, *Guide to Information Technology Security Services*, October 2003.

NIST SP 800-36, *Guide to Selecting Information Security Products*, October 2003.

NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, May 2004.

NIST SP 800-38A, *Recommendation for Block Cipher Modes of Operation — Methods and Techniques*, December 2001.

NIST SP 800-40, *Procedures for Handling Security Patches*, September 2002.

NIST SP 800-41, *Guidelines on Firewalls and Firewall Policy*, January 2002.

NIST SP 800-42, *Guideline on Network Security Testing*, October 2003.

NIST SP 800-43, *Systems Administration Guidance for Windows 2000 Professional*, November 2002.

NIST SP 800-44, *Guidelines on Securing Public Web Servers*, September 2002.

NIST SP 800-45, *Guidelines on Electronic Mail Security*, September 2002.

NIST SP 800-46, *Security for Telecommuting and Broadband Communications,* September 2002.

NIST SP 800-47, *Security Guide for Interconnecting Information Technology Systems*, September 2002.

NIST SP 800-48, *Wireless Network Security: 802.11, Bluetooth, and Handheld Devices,* November 2002.

NIST SP 800-49, *Federal S/MiME V3 Client Profile*, November 2002.

NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program,* October 2003.

NIST SP 800-51, *Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme,* September 2002.

NIST SP 800-55, *Security Metrics Guide for Information Technology Systems*, July 2003.

NIST SP 800-59, *Guideline for Identifying an Information System as a National Security System*, August 2003.

NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, June 2004.

NIST SP 800-61*, Computer Security Incident Handling Guide*, January 2004.

NIST SP 800-64, *Security Considerations in the Information System Development Life Cycle,* October 2003.

Draft SP

DRAFT NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*, October 31, 2003.

United States Department of Health and Human Services Resources

HHS-Information Resources Management (IRM)-2000-0001, *HHS IRM Policy for Capital Planning and Investment Control*, January 8, 2001.

HHS-IRM-2000-0001-GD, *HHS IRM Guidelines for Capital Planning and Investment Control*, January 8, 2001.

HHS-IRM-2000-0004, *HHS IRM Policy for Use of Broadcast Messages, Spamming and Targeted Audiences*, January 8, 2001.

HHS-IRM-2000-0005, *HHS IRM Policy for Information Technology (IT) Security for Remote Access*, January 8, 2001.

HHS-IRM-2000-0006, *HHS IRM Policy for Establishing an Incident Response Capability*, January 8, 2001.

HHS-IRM-2000-0007, *HHS IRM Policy for Prevention, Detection, Removal and Reporting Of Malicious Software*, January 8, 2001.

HHS-IRM-2000-0008, *Domain Names*, January 8, 2001.

HHS-IRM-2000-0009, *HHS IRM Policy for Usage of Persistent Cookies*, January 8, 2001.

HHS-IRM-2000-0010, *HHS IRM Policy for Active Directory*, January 8, 2001.

HHS-IRM-2000-0011, *HHS IRM Policy for Public Key Infrastructure (PKI)*; *Certification Authority (CA),* January 8, 2001.

HHS-IRM-2000-0012, *HHS IRM Policy for Directory Services Using Lightweight Directory Access Protocol (LDAP)*, January 8, 2001.

HHS-IRM-2002-0001, *HHS IRM Policy for Government Emergency Telecommunication System Cards Ordering, Usage and Termination*, November 25, 2002.

HHS-IRM-2003-0001, *HHS IRM Policy For Comments From And Responses To Operating Divisions On Newly Developed Policies and CIO Council and ITIRB Clearance Documents*, February 14, 2003.

HHS-IRM-2003-0002, *HHS IRM Policy for Conducting Information Technology Alternatives Analysis*, supersedes 2000-0002, June 13, 2003.

HHS-IRM-2004-0001, *HHS IRM Policy for Personal Use Of Information Technology Resources*, November 23, 2004

Appendix C: Acronyms

ASAM	Assistant Secretary for Administration and Management
C&A	Certification and Accreditation
CA	Certification Authority
CFR	Code of Federal Regulations
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CIPC	Critical Infrastructure Protection Coordinator
CISO	Chief Information Security Officer
CNSS	Committee for National Security System
CO	Contracting Officer
CPIC	Capital Planning and Investment Control
CSO	Chief Security Officer
CSRC	Computer Security Resource Center
CVE	Common Vulnerability and Exposures
DAA	Designated Approving Authority
DBMS	Database Management System
DoS	Denial of Service
DR	Disaster Recovery
E.O.	Executive Order
FedCIRC	Federal Computer Incident Response Center
FEMA	Federal Emergency Management Agency
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act of 2002
FPC	Federal Preparedness Circular
FRP	Federal Response Plan
GAO	Government Accountability Office
GSS	General Support Systems
HHS	Department of Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act of 1996
Hspd	Homeland Security Presidential Directive
I&A	Identification and Authentication
IA	Information Assurance
IDS	Intrusion Detection System
IIF	Information in Identifiable Form
INFOSEC	Information Security
IP	Internet Protocol
IPSO	Information Processing Service Organization
IRM	Information Resources Management
IRT	Incident Response Team
IS	Information System
ISP	Internet Service Providers
ISSO	Information Systems Security Officer
IT	Information Technology
ITIRB	Information Technology Investment Review Board
ITU	Information Technology Utilities

LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
M	Memoranda
MA	Major Application
MISPC	Minimum Interoperability Specification for PKI Components
MOVS	Modes of Operation Validation System
NARA	National Archives and Records Administration
NCSC	National Computer Security Center
NIACAP	National Information Assurance Certification and Accreditation Process
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OIRM	Office of Information Resource Management
OITSDI	Office of Information Technology Security Development and Implementation
OMB	Office of Management and Budget
OPDIV	Operating Division
PBX	Private Branch Exchange
PDA	Personal Digital Assistant
PDD	Presidential Decision Directive
PIA	Privacy Impact Assessment
PKI	Public Key Infrastructure
POA&M	Plan of Action and Milestones
SANS	System Administration, Networking, and Security Institute
SBU	Sensitive But Unclassified
SLC	System Life Cycle
SOCC	Secure One Communications Center
SP	Special Publication
SSP	System Security Plan
ST&E	Security Testing and Evaluation
STAFFDIV	Staff Division
TMOVS	Modes of Operation Validation System for the Triple Data Encryption Algorithm
USC	US Code
UserID	User Identification
VPN	Virtual Private Network

Appendix D: Glossary

Access — ability to make use of any information system (IS) resource (Defined in National Institute of Standards and Technology [NIST] Special Publication [SP] 800-32, Section 9).

Access Control — enable authorized use of a resource while preventing unauthorized use or use in an unauthorized manner (Defined in NIST SP 800-27, Appendix B).

Accountability — the security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports non-repudiation, deterrence, fault isolation, intrusion detection and prevention, and after action recovery and legal action (NIST SP 800-30, Revision (Rev) A, Appendix E).

Accreditation — the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed upon set of security controls. (Defined in NIST SP 800-37, Appendix B).

Audit — a formal (usually independent) review and examination of a project or project activity for assessing compliance with contractual obligations.

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 trails may apply to information in an information system, input/output media controls, message routing in a communications system, the transfer of communications security material, or a record showing who has accessed a system. In conjunction with appropriate tools and procedures, audit trails can provide a means to accomplish several security-related objectives, including individual accountability, reconstruction of events, intrusion detection, and problem identification. (See the description for Audit Trails as provided in NIST SP 800-14, Section 3.13.)

Authentication — verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system. (Defined in Draft NIST 800-37, Appendix B).

Authorization — the granting or denying of access rights to a user, program, or process (Defined in NIST SP 800-27, Appendix B).

Authorizing Official — official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals. Also known as Designated Approving Authority or Designated Accrediting Authority (Defined in Draft NIST 800-37, Appendix B).

Availability — ensuring timely and reliable access to and use of information (Defined in 44 U.S.C., SEC. 3542).

Awareness, Training, and Education — includes (1) awareness programs set the stage for training by changing organizational attitudes towards realization of the importance of security and the adverse consequences of its failure; (2) the purpose of training is to teach people the skills that shall enable them to perform their jobs more effectively; and (3) education is more in-depth than training and is targeted for security professionals and those whose jobs require expertise in IT security (Defined in NIST SP 800-26, Appendix C).

Banner — display on an information system that sets parameters for system or data use.

Best Practices — the processes, practices, or systems identified in public and private organizations that performed exceptionally well and are widely recognized as improving an organization's performance and efficiency in specific areas. Successfully identifying and applying best practices can reduce business expenses and improve organizational efficiency (Defined in Government Accountability Office (*GAO) Assessing Risks and Returns: A Guide for Evaluation Agencies' IT Investment Decision-making*, February 1997).

Certification — a comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. (Defined in NIST SP-37, Appendix B).

Certification Authority (CA) — the individual, group, or organization responsible for conducting a security certification. (Defined in Draft NIST SP 800-37, Appendix B, Certification Agent).

Confidentiality — preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. (Defined in 44 U.S.C., SEC. 3542).

Contingency Plan — (1) a formal document that establishes continuity of operations processes in case of a disaster. It includes names of responsible parties to be contacted, data to be restored, and location of such data. (2) Management policy and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disaster (Defined in NIST SP 800-34, Appendix E).

Critical Assets — those physical and information assets required for the performance of the site mission.

Critical Infrastructure — physical and cyber-based systems essential to the minimum operations of the economy and government (Defined in PDD-63).

Critical Infrastructure Protection (CIP) — 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.

Data — programs, files or other information stored in, or processed by, a computer system.

Data Integrity — the property that data has not been altered in an unauthorized manner. Data integrity covers data in storage, during processing, and while in transit (Defined in NIST SP 800-27, Appendix B).

Database — a set of related files that is created and managed by a database management system (DBMS).

Department-Wide Information Security Program — HHS is required to develop and implement an information security program for the entire Department, including all Operating Divisions. This program must provide information security for the operations and assets of the Department, including operations and assets provided or managed by another Department (Defined in the *Government Information Security Reform Act of 2000*, section 3534 (b)(1)).

Destruction — the physical alteration of IT media or of IT components such that they can no longer be used for storage or information retrieval.

Encryption — cryptographic transformation of data (called "plaintext") into a form (called "cipher text") that conceals the data's original meaning to prevent it from being known or used. (Defined by System Administration, Networking, and Security Institute [SANS] at http://www.sans.org/resources/glossary.php#A).

Extranet — a network used to communicate with business partners and/or the public.

Facility — a physically definable area consisting of a controlled space that contains national security or sensitive but unclassified (SBU) information processing equipment.

Gateway — interface that provides compatibility between networks by converting transmission speeds, protocols, codes, or security measures.

General Support System (GSS) — an interconnected set of information resources under the same direct management control, which shares common functionality. A GSS normally includes hardware, software, information, data, applications, communications, and people. A GSS can be, for example, a local area network (LAN)

including smart terminals that supports a branch office, an agency-wide backbone, a communications network, a departmental data processing center including its operating system and utilities, a tactical radio network, or a shared information processing service organization (IPSO) (Defined in Office of Management and Budget [OMB] Circular A-130, (A)(2)(c)).

Incident — a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security (defined in NIST SP 800-61, Appendix D).

Information — any communication or representation of knowledge such as facts, data, or opinions in any medium or form; including textual, numerical, graphic, cartographic, narrative, or audiovisual forms (Defined in OMB Circular A-130, 6(a)).

Information Assurance (IA) — measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. (Committee for National Security System [CNSS] Instruction 4009).

Information Resources — information and related resources, such as personnel, equipment, funds, and information technology (Defined in 44 U.S.C., SEC. 3502).

Information Security (INFOSEC) — the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability (44 U.S.C., SEC. 3542).

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. Equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment, or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources (Defined in 40 U.S.C., SEC. 1401).

IT Investments — IT resources that are implemented to strengthen and improve the organization's strategic objectives and business plans while reducing cost.
Integrity — guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity (Defined in 44 U.S.C., § 3542).

Intranet — an internal network intended for HHS only use.

Label — marking an item of information to reflect its security classification.
(a) Internal Label. Marking 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 or cover of the medium that reflects the classification of the information resident within the medium.

Local Area Network (LAN) — a group of computers and associated devices that share a common communications line or wireless link and typically share the resources of a single processor or server within a small geographic area (for example, within an office building) (Defined in NIST SP 800-46, Glossary).

Major Application (MA) — an application that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. (Defined in OMB Circular A-130)

Malicious Code — software (e.g., Trojan horse) that appears to perform a useful or desirable function, but actually gains unauthorized access to system resources or tricks a user into executing other malicious logic. (Defined by SANS at http://www.sans.org/resources/glossary.php#A).

Management Controls — the security controls (i.e., safeguards and countermeasures) applied to an information system that focus on the management of risk and the management of the information security system. Actions that are performed primarily to support management decisions with regard to information system security (Defined in NIST SP 800-53, Appendix B).

Media — all materials in which data and/or information may be stored and it may include floppy disks, CD-ROMs, hard drives, software manuals, and papers.

National Security System — any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency— (i) the function, operation, or use of which: involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions (excluding a system that is to be used for routine administrative and business applications, for example, payroll, finance, logistics, and personnel management applications); or, (ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy (Defined in 44 U.S.C., SEC. 3542).

Need to Know — the necessity for access to or knowledge of 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 manual, such networks are: (a) under the operational control of an HHS official, (b) used for the transmission of classified or SBU data, and (c) may provide connectivity among information systems operated by various classified or SBU information components. Networks include wide- and local-area technologies.

Operational Controls — the security controls (i.e., safeguards and countermeasures) applied to an information system that are primarily implemented and executed by people (as opposed to the information system) (Defined in NIST SP 800-53, Appendix B).

Patch Management — the process of acquiring, testing, and distributing patches to the appropriate administrators and users throughout the organization (Defined in NIST SP 800-61, Appendix D).

Personally Identifiable Information — information in an IT system or online collection: (1) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.), or (2) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors). (Defined in OMB M-03-22).

Personnel Security — the procedures established to ensure that all personnel who have access to sensitive information have the required authority as well as appropriate clearances (Defined in National Computer Security Center [NCSC]-TG-004).

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 or lower category as the level of the personnel security clearance being granted.

Physical Security — the application of physical barriers and control procedures as preventive measures or countermeasures against threats to resources and sensitive information (Defined in NCSC-TG-004).

Plan of Action and Milestones (POA&M) — a document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones (Defined in OMB Memorandum 02-01).

Policy — the rules and regulations set by an organization that define the purpose of the program and its scope within an organization; assigns responsibilities for direct program implementation, as well as other responsibilities to related offices (e.g.,

Chief Information Office); and addresses compliance issues. A program policy sets organizational and strategic directions for security and assigns resources for its implementation (Defined in NIST 800-12).

Privacy Impact Assessment (PIA) — an analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks (Defined in OMB M-03-22).

Residual Risk — the portion of risk remaining after the application of appropriate security controls in the information system (Defined in Draft NIST SP 800-37, Appendix B).

Risk — the level of impact on agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring (NIST SP 800-30, Rev A, Appendix E).

Risk Assessment — the process of identifying risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals by determining the probability of occurrence, the resulting impact, and additional security controls that would mitigate this impact. Part of risk management, synonymous with risk analysis, and incorporates threat and vulnerability analyses (NIST SP 800-30, Rev A).

Risk Management — the process of managing risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system. It includes: risk assessment; cost-benefit analysis; the selection, implementation, and assessment of security controls; and the formal approval to operate the system. The process considers effectiveness, efficiency, and constraints due to laws, directives, policies, or regulations (NIST SP 800-30, Rev A).

Rules of Behavior — the rules that have been established and implemented concerning use of, and security in, 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 (Defined in NIST SP 800-18, Appendix D).

Sanitization — eliminating sensitive information from an IT system or media associated with an IT to permit the reuse of the IT or media at a lower classification level or to permit the release to unauthorized personnel or personnel without the proper need to know.

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).

Security — the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability (Defined in 44 U.S.C., SEC. 3542).

Security Controls — the management, operational, and technical controls (safeguards or countermeasures) prescribed for an information system which, taken together, adequately protect the confidentiality, integrity, and availability of the system and its information (Defined in NIST SP 800-53, Appendix B).

Security Safeguards — the protective measures and controls 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 Violation — the failure to comply with policy and procedures established by the federal government that could reasonably result in the loss or compromise of sensitive information.

Sensitive Data — information whose loss, misuse, unauthorized access to, modification, or destruction could adversely affect the national interest or the conduct of federal programs, or privacy to which individuals are entitled, but which has not been specifically authorized to be kept secret in the interest of national defense or foreign policy, etc. Sensitive data can relate to industry (e.g., proprietary, patented), copyrighted or business data, as well as data that is simply inappropriate for public release.

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; these levels of required protection are 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.

Separation of Duties — the practice of dividing roles and responsibilities so that a single individual does not control the entirety of a critical process (Defined in NIST SP 800-12).

Session — The period of time a user interfaces with an application. The user session begins when the user accesses the application and ends when the user quits the application.

System — (1) a collection of components (hardware, software, and interfaces) organized to accomplish a specific function or set of functions; generally considered a self-sufficient item in its intended operational use.

System Life Cycle (SLC) — a formal model of a hardware or software project that depicts the scope of and relationship among activities, products, reviews, approvals, and resources. In addition, the period that begins when a need is identified (initiation) and ends when a system ceases to be available for use (disposition). Note: Activities associated with a system include the system's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal (that may instigate another system initiation) (Defined in NIST SP 800-34, Appendix E).

System Security Plan (SSP) — formal document that provides an overview of the security requirements of the information system and describes the security controls in place or planned for meeting those requirements (Defined in NIST SP 800-53, Appendix B, Security Plan).

Technical Controls — the security controls (i.e., safeguards and countermeasures) applied to an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system (Defined in NIST SP 800-53, Appendix B).

Threat — any circumstance or event with the potential to intentionally or unintentionally exploit a specific vulnerability in an information system resulting in a loss of confidentiality, integrity, or availability (Defined in NIST SP 800–53, Appendix B).

Unauthorized Disclosure — exposure of information to individuals not authorized to receive it.

User — person or process accessing an information system either by direct connections (that is, by way of terminals), or indirect connections (that is, prepare input data or receive output that is not reviewed for content or classification by a responsible individual).

Validation — the process of determining the correctness of the final product, system, or system component for the user's requirements. Answers the question, "Am I building the right product?"

Verification — the process used by an independent agent to confirm or establish by testing, evaluation, examination, investigation, or competent evidence, the effectiveness of the security controls in an information system (Defined in NIST SP 800–53, Appendix B).

Vulnerability — a flaw or weakness in the design or implementation of an information system (including the security procedures and security controls

associated with the system) that could be intentionally or unintentionally exploited to adversely effect an organization's operations or assets through a loss of confidentiality, integrity, or availability (Defined in NIST SP 800-53, Appendix B).

Vulnerability Assessment — formal description and evaluation of the vulnerabilities in an information system (CNSS Instruction 4009).

Appendix E: Information Security Program Documents

The Department of Health and Human Service (HHS) Information Security Program is supplemented by a series of HHS Information Security documents. These documents include:

- HHS Information Security Program Policy
- HHS Information Security Program Handbook
- HHS Information Security Program Rules of Behavior
- Baseline Security Requirements Guide
- Certification and Accreditation (C&A) Guide
- Configuration Management Guide
- Contingency Planning for Information Security Systems Guide
- Critical Infrastructure Protection (CIP) Planning Guide
- Data Cryptography Guide
- Disaster Recovery Planning Guide
- Firewall Configuration Guide
- Health Insurance Portability and Accountability Act (HIPAA) Compliance Guide
- Incident Response Planning Guide
- Information Privacy Program Policy
- Information Privacy Program Handbook
- Information Technology (IT) Penetration Testing Guide
- IT Personnel Security Guide
- IT Physical and Environmental Security Guide
- IT Privacy Impact Assessment Guide
- IT Security Capital Planning Guide
- Machine-Readable Privacy Policy Guide
- Plan of Actions and Milestones (POA&M) Guide
- Risk Assessment Guide
- Security Test and Evaluation (ST&E) Planning Guide
- Web Security Guide
- Wireless Security Program Development Guide

Appendix F: Departmental Policy Waiver

Departmental Policy Waiver

Date:_____

Agency Name:_____

Agency Requester Name:_____

Phone Number:_____

Departmental Policy: _____

Justification for noncompliance or deviation:_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____ _____

Agency Representative Signature Date

_____ _____

Agency Chief Security Officer (CSO) Date

Acknowledgements

Carlos Figueroa, Steven Friend, Terri Hall, Meighan O'Rearadon, Phil Shea and Jonathan Smith were instrumental in the development of this document.