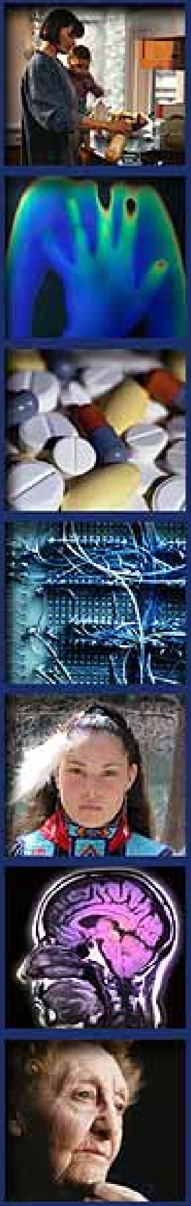

Information Security Program

Information Security Program Handbook

December 1, 2005

FOR OFFICIAL USE ONLY
This information is intended for HHS use only. Disclosure is not expected to cause serious harm to HHS, and access is provided freely to all internal users via the organization's intranet.

SECURE ONE HHS
KEEP AMERICA'S HEALTH AND HUMAN SERVICES SECURE

DISCLAIMER: This document is for official use only[1] and is intended for use by the United States Department of Health and Human Services (HHS), including all of its Operating Divisions (OPDIV) and Staff Divisions (STAFFDIV). Throughout the *HHS Information Security Program Handbook* the terminology “the Department” or “Departmental” includes all HHS, OPDIV, and STAFFDIV personnel, contractors, and other authorized users.

The procedures outlined *in the Information Security Program Handbook* are not mandatory for the Department to follow. They are, however, best practices and will provide guidance to the Department in meeting or exceeding the mandatory policies identified in the *Information Security Program Policy* document.

[1] Disclosure of this handbook is not expected to cause serious harm to HHS, and access is provided freely to all internal users and contractors via the organization’s intranet.

Table of Contents

Preface

The Department of Health and Human Services (HHS) is pleased to present this *Information Security Program Handbook*. This handbook and the companion *HHS Information Security Program Policy* are the foundation documents for the Department's Information Security Program. These documents implement relevant federal laws, regulations, and policies at the Department and provide a basis for the information security policies for the Department. Specific information listed in this document is further detailed in the subject-specific HHS Information Security Program guides.

As the HHS Information Security Program evolves, this document is subject to review and revision. Review and update will take place annually, or when changes occur that identify the need to revise the *HHS Information Security Program Handbook*. This may include:

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

The responsibility for maintaining and updating this policy is delegated to the HHS Chief Information Security Officer (CISO). All revisions should be highlighted in the Document Change History table. When finalized, new versions of this *HHS Information Security Program Handbook* should be disseminated throughout the Department.

Document Change History

Version Number	Release Date	Summary of Changes	Section Number / Paragraph Number	Changes Made By
1.0	07/30/2004	Initial Draft Document Release	NA	NA
2.0	11/10/2004	Final Document Release	NA	NA

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, the Department has instituted the *HHS Information Security Program Policy* and developed the accompanying *HHS Information Security Program Handbook*.

The *HHS Information Security Program Handbook* provides comprehensive, uniform information security procedures to be followed by the Department. Each topic in this handbook contains a procedures section that provides an approach for compliance with the requirements imposed on the Department. Additionally, there is a reference section for each topic that identifies other documents that provide additional guidance.

1.1 Scope and Applicability

The HHS Information Security Program provides an integrated and comprehensive approach to securing Departmental information systems. The keystone of the program is the *HHS Information Security Program Policy* and the *HHS Information Security Program Handbook*. These documents provide direction to the Department in the form of policies, standards, and guidelines. The handbook provides the procedures and guidance to the Department to meet or exceed the policies and standards set in the policy document. The handbook applies to all Departmental personnel, contractors, and authorized users who access Departmental information systems and is also applicable to all Departmental information systems used to process, store, transmit, or receive Departmental data of any sensitivity or classification, regardless of when or how they were acquired or where they are operated.

1.2 Reference Guidance Documents

A series of HHS-related guides has been created to further detail the procedures outlined for specific functions of the HHS Information Security Program. A list of these guides can be found in appendix E.

1.3 Document Organization

The procedures outlined in this handbook are subdivided into the same three major security control areas (i.e., management, operational, and technical) as the policy document. For easy reference, section numbers within this document are organized to correspond with those in the *HHS Information Security Program Policy*.

The structure for the remainder of the document is as follows:

- Section 2 provides an overview of the handbook and identifies the key personnel involved in implementing an information security program.
- Section 3 provides the mandatory standards and procedures relating to management controls.
- Section 4 provides the mandatory standards and procedures relating to operational controls.
- Section 5 provides the mandatory standards and procedures relating to technical controls.
- Appendix A provides a feedback form to submit comments on the document.
- Appendix B lists the references used in this document.
- Appendix C lists the acronyms used in this document.
- Appendix D defines the terms most frequently used in this document.
- Appendix E provides a list of the guidance documents associated with the HHS Information Security Program.
- Appendix F contains a non-disclosure agreement for contractors working for the Department to sign.
- Appendix G contains the Departmental Rules of Behavior for all users to sign.
- Appendix H contains a checklist to support the separation process for Departmental personnel.
- Appendix I contains a cleaning and sanitization matrix.
- Appendix J includes a checklist to assist staff with electronic media disposal.
- Appendix K provides examples of warning banners.
- Appendix L contains a matrix of services blocked using the firewall.

2. Overview

This handbook presents the procedures that are required when implementing the policies found in the *HHS Information Security Program Policy* document. The handbook establishes procedures that relate to management, operational, and technical security controls that provide the foundation for ensuring confidentiality, integrity, and availability within the Department's information technology (IT) infrastructure and operations.

2.1 Key Personnel

Departmental personnel ranging from executive level to system level play integral roles in implementing a successful Information Security program. The list below illustrates the key personnel involved.

- Secretary of HHS
- Department Leadership

    1. HHS Chief Information Officer (CIO)
    2. OPDIV Heads
    3. Deputy Assistant Secretary for Finance
    4. Assistant Secretary for Administration and Management
    5. Deputy Assistant Secretary for Human Resources

- Information Security Leadership

    1. HHS Chief Information Security Officer (CISO)
    2. OPDIV CIOs
    3. OPDIV CISOs
    4. HHS Information Systems Security Officer (ISSO)
    5. OPDIV ISSOs

- Information Security Roles

    1. Designated Approving Authority (DAA)
    2. Certification Authority (CA)
    3. Program executives
    4. Critical Infrastructure Protection Coordinator
    5. Contingency Planning Coordinator
    6. System owners
    7. Data owners
    8. System/Network administrators
    9. Contracting officers
    10. Personnel officers
    11. Supervisors
    12. Users and employees

- Department Security Council

1. Information Technology Investment Review Board

The specific responsibilities for these roles are identified in the *HHS Information Security Program Policy* document.

3. Management Controls

3.1 Capital Planning and Investment Control

Procedures

- Establish a process to review business cases and budget requirements for achieving adequate IT security for each IT capital investment.
- Ensure that security requirements for the applications supporting their programs are adequately resourced.
- Ensure that costs—dollars or personnel requirements—are associated and tracked with identified security vulnerabilities.
- Incorporate inputs from the HHS IT Security Performance Measurement Program into the IT security capital planning process.
- Use consistent methodologies for identifying IT security costs.

    1. It is not acceptable to determine IT security costs using a fixed percentage of total cost; methodologies are subject to the review and approval of the HHS CISO.

- Integrate IT security cost data with system inventories.
- Ensure that the security planning process assists in selecting cost-effective safeguards that reduce risks to an acceptable level prior to implementation of the system.

    1. The benefit is to minimize expenditure of funds and staff resources for security. Evaluating risks after a production status and backtracking security controls into a production status system is wasteful of limited resources.

- Enforce guideline that all IT procurement requires a security consideration review and OPDIV CISO approval.

References

OMB Circular A-130, Appendix III; Public Law (P.L.) 107-347 Title III, FISMA; OMB Memorandum 97-02, *Funding Information Systems Investments*; National Institute of Standards and Technology (NIST) Special Program (SP) 800-9, *Good Security Practices for Electronic Commerce;* OMB Memorandum 00-07, *Incorporating and Funding Security in Information Systems Investments*; OMB Memorandum 97-16, *Information Technology Architectures*; *Information Technology Management Reform Act* (Clinger-Cohen Act).

Refer to the *HHS IT Security Capital Planning Guide* for further guidance.

3.2 Contractors and Outsourced Operations

Procedures

- Review all contracts before they are awarded to ensure IT security requirements have been incorporated.
- Ensure that at the expiration of a contract, contractors erase Departmental information from any contractor-owned system used to process information and return any Departmental IT resources provided to them.
- Ensure appropriate policies and procedures on activities of external third parties (e.g., service bureaus, contractors, other service providers such as system development, network management, security management) are documented (e.g., for all contractors using Departmental systems ensure they sign the Departmental Non-Disclosure Agreement, and comply with Departmental security policies), agreed to, implemented, and monitored for compliance and include provisions for the following:

    1. security clearances (where appropriate and required)
    2. background checks
    3. required expertise
    4. confidentiality agreements
    5. security roles and responsibilities
    6. connectivity agreements
    7. individual accountability.

- Develop and implement an IT security contract clause to be enforced against all relevant Departmental contracts.
- Write specialized security requirements into the contract statements of work or professional services contracts.

    1. The HHS CISO should work with the Assistant Secretary of Administration and Management in accomplishing this requirement.

- Conduct an annual security review when work is performed at the contractor’s facility.
- Require outsourced operations, where non-Departmental personnel have access to government information and critical Departmental systems and network components, comply with the security required by Federal Acquisition Regulation (FAR) clause 52.239-1, *Privacy or Security Safeguards.*

References

NIST SP 800-36, *Guide to Selecting Information Technology Security Products*; NIST SP 800-35, *Guide to Information Technology Security Services*; NIST SP 800-4A, *Security Considerations in Federal Information Technology Procurements*; NIST SP 800-47, *Security Guide for Interconnecting Information Technology Systems*.

Refer to the *HHS IT Personnel Security Guide* for further guidance.

Refer to appendix F for a Non-Disclosure Agreement form.

3.3 Security Performance Measures and Metrics

Procedures

- Report those performance measures defined by Congress and OMB in accordance with FISMA for inclusion in the Departmental program.
- Establish five to ten internal security metrics of high data quality, as defined by OMB, to track the progress of the security program.

  1. The OPDIV CISOs and program officials should identify these metrics, in addition to mandated measures collected under legislative, OMB, and Office of the Inspector General (OIG) review. Metrics will be linked to the HHS IT Performance Plan.

- Define annually the required measures and associated performance goals that are common to the Department.
- Report metrics from staff to the executive level. System owners are responsible for reporting metrics to their OPDIV CISOs, who will in turn report the metrics to the HHS CISO.

References

NIST SP 800-55, *Security Metrics Guide for IT Systems*.

For additional guidance, please see OMB Guidelines for *Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of Information Disseminated by Federal Agencies*, January 2002.

3.4 Critical Infrastructure Protection Support

Procedures

- Establish and document a critical infrastructure protection (CIP) program and plan using the following procedures:

  1. Issue guidance on protecting critical IT infrastructure assets, including major applications (MA) and general support systems (GSS) (as defined by OMB A-130, Appendix III) and vital records.
  2. Establish and document a Department-wide process to identify and prioritize critical infrastructure, the interdependent and dependent relationships, protection concerns, and protection solutions.
  3. Implement a centralized reporting system for critical asset management.
  4. Perform analysis and vulnerability assessments of all Departmental IT critical assets yearly (at a minimum).

5. Make certain vital records are protected to ensure continuity of operations and to protect the legal and financial rights of the Department and persons affected by the Department.
6. Establish necessary public and private sector partnerships as a means of reducing shared risk and coordinating Departmental critical infrastructure requirements.

References

E.O. 13231, *Critical Infrastructure Protection in the Information Age*; Homeland Security Presidential Directive (Hspd)-7, *Critical Infrastructure Identification, Prioritization, and Protection.*

Refer to the *HHS Critical Infrastructure Protection Planning Guide* and the *HHS Incident Response Planning Guide* for further guidance.

3.5 System Life Cycle

Procedures

- Perform an assessment as early as possible in the system life cycle (SLC) to determine the sensitivity and criticality of and possible threats to the system and of the information to be processed.
- Develop system security requirements as a collaborative effort between system owners and security certifiers.
- Ensure that an initial system security plan (SSP) is drafted, integrating the security requirements of the system.
- Configure and enable system security features before a system is tested or enters production.
- Implement policies and procedures to assure that authorizations for software modifications are documented and maintained.
- Remove any systems in need of retirement while resolving final disposition issues and concerns and addressing legal considerations for retention of Departmental records.
- Implement policies and procedures to ensure record keeping that documents who implements media disposal and verifies media sanitization.
- Ensure the system receives Certification and Accreditation (C&A) before it enters production (see section 3.14).

References

NIST SP 800-37,*Guide for the Security Certification and Accreditation of Federal Information Systems;* NIST SP 800-64, *Security Considerations in the Information System Development Life Cycle*.

Refer to the *HHS Certification and Accreditation Guide* for further guidance.

3.6 Change Management Control

Procedures

- Establish, implement, and enforce configuration management plans and change management controls by:

  1. Ensuring that the configuration management procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and HHS guidelines and is evaluated periodically—at least annually—to verify the plan and the ability of those tasked to carry out the plan.
  2. Ensuring that scheduled changes to the information system are authorized by appropriate organization Change Control Board (CCB) prior to implementation and are not permitted outside of the configuration management process.
  3. Ensuring that emergency changes (unscheduled changes such as mitigating new discovered security vulnerabilities, system crashes, replacement of broken down critical hardware components, etc.) are authorized by the appropriate organization CCB as soon as possible after the emergency change is implemented.
  4. Training personnel involved in configuration management with the Departmental configuration management process.
  5. Requiring the use of appropriate tools to produce audit trails of program changes, maintain program version numbers, record and report program changes, maintain creation/date information for production modules, maintain copies of previous versions, and control concurrent updates.
  6. Evaluating the impact on the security posture for all proposed changes to an IT system, including security patches.
  7. Evaluating and testing changes made to a system during development or after deployment to ensure that the changes do not adversely affect any of the security properties of the system.
  8. Requiring that configuration management plans include processes that permit review and recommendation by the system Certification Authority (CA).

- Ensure production program changes are periodically reviewed by appropriate organization officials to determine whether access controls and change controls are being followed.
- Review the baseline security requirements to establish configuration management and security change management plans for all IT systems and major networks.
- Assess cost and impact of all planned (i.e., installation of new technologies) and unplanned changes (i.e., maintenance, upgrades, or fine-tuning) for each IT system or network before implementation.
- Develop methods of evaluating, approving, and installing security patches to ensure that they comply with configuration management plan and that they can be implemented in a timely manner.

- Notify all system users of system outage before all planned changes to all IT systems and major networks.
- Notify all system users of system outage during unplanned changes to all IT systems and major networks.
- Implement controls to monitor and document installations, updates, and modifications to all IT systems and networks; these records shall be kept for at least one year.

References

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

Refer to the *HHS Configuration Management Guide* and the *HHS Certification and Accreditation Guide* for further guidance.

3.7 Risk Management

Procedures

- Assess risk when a system is developed or updated and perform risk assessments whenever there is a significant modification to the IT system or, if there have been no significant modifications, every three years.
- Work with OPDIV CISOs to certify and accredit systems.

    1. Based on the C&A analysis, the DAA will evaluate the acceptance of residual risk or implement countermeasures.

- Document the acceptance of the risk and the justification for the decision in the Risk Assessment report.

    1. The system owner should maintain the Risk Assessment report and all C&A documentation with a file copy to the OPDIV CISOs.

- Ensure that the Risk Assessment process includes these activities:

    1. **System Characterization.** This activity establishes the scope of the risk assessment effort and provides information essential to defining the risk. This information includes information infrastructure, hardware, data and information, people, and system interfaces and connectivity.
    2. **Threat Identification.** This activity identifies realistic threats; potential natural, environmental, and human threats; and threat-sources. Advisories, interviews, incident reports, and other sources are used as resources to determine potential threats.

    3. **Vulnerability Identification.** This activity evaluates threats in the context

of the system characterization to determine how HHS systems are exposed to the identified vulnerabilities.

4. **Level of Risk Determination.** This activity determines the impact of an incident against the likelihood of threat occurrence.
5. **Risk Mitigation.** This activity eliminates threats or implements security controls to minimize the impact of a threat.
6. **Acceptance of Risks.** This activity entails the DAA's acceptance of the current security controls and known risks to the system.

- Integrate a risk-management process throughout all development stages of MAs and GSSs.
- Conduct risk analyses using commercial software or through a comprehensive qualitative or quantitative analysis.
- Perform a review of security controls using NIST SP 800-26 and NIST SP 800-30 or equivalent risk mitigation review process.

1. For new systems, this review should happen prior to design approval and for existing systems every three years at minimum.

- Implement a risk-management process to assess the risks to information resources and systems in the Department.

1. The principal goal of the Department's risk-management process is to ensure the protection of the organization, its ability to perform mission requirements, and protect its systems and data. In addition, the risk-management procedures and processes should balance the operational and economic costs of protective measures and improve mission capabilities by protecting its systems and data.

- Integrate risk-management concepts into the SLC to address risks in uncovered areas in each phase of the system's life cycle, including initiation, development or acquisition, implementation, operation or maintenance, and disposal.
- Implement risk-mitigation strategies for each system to address the prioritization, evaluation, and implementation of effective risk-reduction controls.
- Ensure consideration of the minimum risk mitigation options of risk assumption, avoidance, limitation, planning, research and acknowledgment, and transference.
- Revise risk assessment policies and procedures, as required, to assure that risk assessments are performed and documented regularly or whenever the system, facilities, or significant modifications are made.

References

Federal Information Processing Standard (FIPS) Publication (PUB) 31, *Guidelines for Automatic Data Processing Physical Security and Risk Management*; NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook;* NIST SP 800-26, *Security Self-Assessment Guide for Information Technology Systems;* NIST SP 800-30, *Risk Management Guide for Information Technology Systems*.

Refer to the *HHS Risk Assessment Guide* and the *HHS Certification and Accreditation Guide* for further guidance.

3.7.1 Security Program Review

Procedures

- Conduct program reviews annually in accordance with OMB guidance.
- Collect security program performance measurements required for submission to OMB.

References

FISMA; NIST SP 800-18, *Guide for Developing Security Plans*; NIST SP 800-26, *Security Self-Assessment Guide for Information Technology Systems*;
NIST SP 800-30, *Risk Management Guide for Information Technology Systems*;
and OMB Circular A-130.

3.7.2 Security Control Review

Procedures

- Review security controls in place for MAs and GSSs at least annually or when a significant modification occurs within an MA or GSS.

    1. The review shall evaluate the security control areas to assess whether they are functioning properly, identify vulnerabilities that could heighten threats to sensitive, mission-critical, high-investment systems or resources, and assist with implementing new safeguards where required. The reviews are part of internal control reviews conducted in accordance with OMB Circular A-123 and should:

        a. Evaluate the adequacy of the application’s security controls.
        b. Ensure that controls are functioning properly.
        c. Identify any new or increased vulnerability.
        d. Formulate plans for implementing revised security controls.

References

FISMA; NIST SP 800-18, *Guide for Developing Security Plans for Information Technology Systems;* NIST SP 800-26, *Security Self-Assessment Guide for Information Technology Systems;* NIST SP 800-30, *Risk Management Guide for Information Technology Systems;* and OMB Circular A-130, Appendix III.

3.7.3 Risk Assessments

Procedures

- Ensure that the risk assessment is consistent with the intent of NIST SP 800-30 and that the documented risk assessment includes the following:

  1. identification of the conditions for reassessment, indicating the period for periodic reassessment and defining the level of change to the information system or environment that will cause a reassessment to occur
  2. identification of the security authorization boundary
  3. configuration of the current information system, including connections to other systems
  4. actions that will be taken to ensure that the boundary definition is accurately updated periodically
  5. an inventory of information system assets
  6. identification and assessment of threat sources
  7. identification and assessment of information system vulnerabilities
  8. identification of risks from third-party connections.

- Revise risk assessment policies and procedures, as required, to assure that risk assessments are performed and documented regularly or whenever the system, facilities, or significant modifications are made.
- Ensure that the risk-assessment process considers and addresses data sensitivity and integrity.
- Ensure that the risk-assessment process identifies potential threat sources, both natural and man-made.
- Develop a list of known system vulnerabilities, system flaws, and weaknesses
- Ensure that the risk-assessment process determines whether the security requirements in place adequately mitigate vulnerabilities.
- Implement policies and procedures to provide an effective and timely process for reporting significant weaknesses and ensuring effective remedial action in accordance with FISCAM and NIST SP 800-18.

References

Executive Order (E.O.) 13231; FISMA; NIST SP 800-18, *Guide for Developing Security Plans for Information Technology Systems;* NIST SP 800-26, *Security Self-Assessment Guide for Information Technology Systems;* and NIST SP 800-30, *Risk Management Guide for Information Technology Systems*.

3.7.4 System Interconnectivity/Information Sharing

Procedures

- Ensure authorization to interconnect or share systems or information is in the form of a Memorandum of Understanding (MOU) or Memorandum of Agreement (MOA) and based upon the acceptance of risk to interconnected systems.
- Execute and implement written agreements for data sharing among interconnected systems.
- Ensure that authorization is obtained prior to connecting to or disconnecting from interconnected systems.

References

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

3.8 Privacy Impact Assessments

Procedures

- Complete Privacy Impact Assessments (PIA) and submit through the Information Security Data Management (ISDM) tool.

  1. The Department shall assign the appropriate individuals (e.g., system owners) to complete the PIAs.
  2. Completed PIAs shall be reviewed and approved by the OPDIV Privacy Act Contact, the OPDIV Chief Information Officer, and the OPDIV head.
  3. Submission of PIAs through the ISDM is confirmation of the approval of these individuals and the OPDIV Information Security Officer; however, signed hard copies shall be retained by the OPDIVs in the event of OIG, OMB, or OCIO review.
  4. Once PIAs are submitted, the ISDM system characterization module should be updated to reflect this completion.

References

Clinger-Cohen Act; E-Gov Act, Section 208: FISMA; *Health Insurance Portability and Accountability Act* (HIPAA); NIST SP 800-30, *Risk Management Guide for Information Technology Systems;* OMB Circular A-123; OMB Circular A-130; OMB M-03-22; and *Privacy Act of 1974.*

Refer to the *HHS IT Privacy Impact Assessment Guide* for further guidance.

3.9 Self-Assessments

Procedures

- Conduct self-assessments using NIST Special Publication 800-26, *Security Self-Assessment Guide for Information Technology Systems* on an annual basis to:

    1. Determine if security controls are correctly implemented and, as implemented, are effective in their application.
    2. Ensure that security-applicable laws, executive orders, directives, policies, regulations, standards, and guidelines are met.

- Conduct self-assessments annually to monitor the effectiveness of security controls.

    1. prior to initial operational capability and authorization to operate
    2. prior to each re-authorization to operate
    3. when a significant modification to the information system occurs.

- Conduct and document management reviews of system assessment results to form the basis for management decisions and action plans.
- Retain inspection reports, including self-assessment reports, corrective actions, and supporting documentation for a minimum of five years.

References

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

3.10 Plan of Action and Milestones

Procedures

- Weaknesses found during the security program, security control, risk assessment, privacy impact assessment, and self-assessment reviews shall be documented in a Plan of Action and Milestones (POA&M).
- Each OPDIV and STAFFDIV shall develop and implement a POA&M to manage and track the corrective actions for all systems that support Departmental operations.
- The POA&M shall be consistent with OMB M-02-09 and should include:

    1. all security weaknesses
    2. point of contact
    3. resources required
    4. scheduled completion date
    5. milestones with completion dates
    6. changes to milestones

7. status (i.e., ongoing or completed)
8. financial data linking the security costs for a system with the security performance of a system
9. all security weaknesses found during any other review done by, for, or on behalf of the Department, including General Accounting Office (GAO) or Inspector General (IG) audits, financial system audits, and critical infrastructure vulnerability assessments.

- Each OPDIV and STAFFDIV shall submit each POA&M to the HHS CISO.
- The HHS CISO shall integrate each POA&M into the Department's Master POA&M.
- The Department shall provide OMB with annual reports and quarterly updates on POA&M implementation, including all necessary weakness information.

References

OMB Circular A-123; OMB Circular A-130, Appendix III; P.L. 107-347 Title III, FISMA; OMB Memorandum 02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*; OMB M-03-19, *Memorandum for Heads of Executive Departments and Agencies*, August 2003; OMB Memorandum 02-09, *Reporting Instructions for the Government Information Security Reform Act and Updated Guidance on Security Plans of Action and Milestones;* and NIST SP 800-55, *Security Metrics Guide for Information Technology Systems*.

3.11 System Inventory

Procedures

- Provide information to the HHS CISO on the nature of the system, including the information it processes and any special security requirements.
- Validate inventory for use in Departmental submissions to OMB.

References

Refer to FISMA and the *HHS System Inventory Guide* for additional information.

3.12 System Categorization

Procedures

- Categorize the information system in accordance with FIPS Publication 199 and NIST SP 800-60 such that the security categorization is explicitly documented and approved by an appropriate senior official.

References

FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems, and FISMA.

3.13 System Security Plans

Procedures

- Develop System Security Plans (SSP) for all Departmental MAs and GSSs that are compliant with OMB policy and consistent with guidance provided by NIST SP 800-18; this guideline is required regardless of how the application or system is procured or managed. This guideline also includes all MAs and systems under development and/or outside the Department. In developing and documenting the plan, the following procedures should be followed:

    1. Ensure that the system owner oversees preparation of the plan with support from the developers, system managers, and a system security designee.
    2. Include inputs from interested parties, including end users, system administrators, and the OPDIV CISOs.
    3. Ensure that Rules of Behavior, as defined by OMB Circular A-130, Appendix III, are developed and included in all SSPs.
    4. Ensure a hard and soft copy of the SSP for each GSS is made available to Departmental CIOs, CISOs, ISSOs, and system owners.

- Retain these plans and their associated authorization documents as part of the official agency records and make them available to OMB and NIST for review and comment.
- Review and update the security plan as needed to reflect current conditions, both on a regular basis every year and whenever there are significant changes defined as and authorized to the information system, facilities, or other conditions that may impact security.
- Ensure that the security plan is prepared, implemented, and monitored for its effectiveness.

References

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

3.14 Authorize Processing (Certification and Accreditation)

Procedures

- Certify and accredit all sensitive systems using NIST SP 800-37 guidance for all systems entering the process after July 2004 and continue to use National Information Assurance Certification and Accreditation Process (NIACAP) for those systems that started the process prior to July 2004.
- Ensure the C&A process includes (at a minimum) the following activities:

  1. C&A role determination and assignment
  2. system characterization/description
  3. accreditation boundary determination
  4. system sensitivity determination
  5. security plan (e.g., SSP or SSAA) development and review
  6. initial and continuous risk assessments
  7. security control/requirement determination
  8. implementation of determined security controls/requirements in the system
  9. required security document development
  10. independent security testing and evaluation
  11. certification package preparation
  12. accreditation package preparation
  13. continuous review and monitoring of system changes
  14. re-accreditation.

- Accredit or re-accredit IT systems every three years, or whenever significant changes to the system occur.
- Design systems in development to meet the appropriate level of trust at which it is to be accredited.
- Designate, to the extent it is considered appropriate, program officials as DAAs for their respective offices.

  1. Where an IT system substantially involves more than one DAA, it will be advantageous to mutually agree to a lead-DAA to represent the interests of the other DAAs.

References

NIST SP 800-37, *Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems*; and *National Information Assurance Certification and Accreditation Process (NIACAP)*.

Refer to the *HHS Certification and Accreditation Guide* for further guidance.

3.14.1 Certification

Procedures

- Ensure the CA reviews the C&A packages the system owners/developers provide and recommends acceptance or rejection of risk to the DAA.
- Ensure for each system reviewed, the CA is responsible for delivering a certification package to the DAA that includes, at a minimum:

    1. an SSP with at least the following appendices:

        a. Risk Assessment Report
        b. PIA
        c. Contingency Plan
        d. a Security Assessment Report (e.g., Security Test & Evaluation (ST&E) Report)
        e. an action plan from the system owner and recommendations for corrective actions (e.g., POA&M)
        f. the CA recommendation statement.

- Ensure the CA assures that the ST&E validates both technical and non-technical controls. For example, the CA may want to review any rules of behavior, configuration management plans, contingency/disaster recovery plans, interface control documents, and/or interconnection agreements and may incorporate these documents as part of the accreditation package kept on file.

References

Refer to the *HHS Certification and Accreditation Guide*, the *HHS Configuration Management Guide*, and the *HHS Contingency Planning for Information Security Guide* for further guidance.

3.14.2 Accreditation

Procedures

- Ensure that the accreditation package consists of the certification package and the accreditation decision letter.
- Ensure the DAA gives a full accreditation decision or denies authority to operate.
- Authorize the DAA to grant exceptions to some security requirements based on acceptable risk; in such cases:

    1. The request for an exception should include a statement of the requirements that are to be accepted, the reason that identified requirements cannot be implemented, evidence to support that claim, the acceptable risk, the offsetting countermeasures that are to be substituted in place of the security requirement, and a timetable for completion.

2. The request for an exception should state which aspect of the threat is related to the proposed request and evidence should be submitted that planned countermeasures will allow secure operation of the system at an acceptable level of risk.
3. A plan for implementing the "excepted" security requirements later in the life cycle is developed.
4. Approval of the exception makes it incumbent on the DAA to take the necessary risks, programmatic planning and funding steps to ensure implementation of any security requirements that are postponed temporarily as a consequence of approval of the exception. The approved written exception should be maintained with the accreditation package.

References

Refer to the *HHS Certification and Accreditation Guide* for further guidance.

Policy Waiver

Procedures

a. Determine if implementing any other controls (technical or procedural) limit the risk to a level where additional controls required are unnecessary.
b. Review the cost of implementing a control to determine if it is not commensurate with the protection offered.

References

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

4. Operational Controls

4.1 Personnel Security

4.1.1 Background Investigations

Procedures

- Ensure all personnel meet personnel security and suitability standards commensurate with their position's sensitivity level and are subject to personnel investigation requirements.
- Screen individuals requiring access to information (e.g., verification of background checks and investigations as well as security and non-disclosure agreements) prior to being granted access in accordance with organizational personnel security policies.
- Refuse employees and contractors access to sensitive IT systems until they have a favorably adjudicated background investigation (BI) or have been granted an interim clearance.
- Screen privileged users (i.e., individuals who are authorized to bypass significant technical and operational controls) prior to access and periodically every two years.
- Perform periodic reinvestigations at time intervals consistent with the criticality/sensitivity rating of the position, according to criteria from the Office of Personnel Management (OPM).
- Conduct BIs in a manner commensurate with current OPM and HHS Office of Human Resources (OHR).
- Ensure that personnel in high-risk positions are identified, including:

  1. CISOs
  2. ISSOs
  3. system/network administrators
  4. computer repair technicians
  5. programmers/database administrators
  6. any other position that requires "super-privileges" or the ability to modify applications or sensitive data.

References

OMB Circular A-130, Appendix III; P.L. 107-347 Title III, FISMA; FISCAM; NIST SP 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*; NIST SP 800-18, *Guide for Developing Security Plans for Information Technology Systems*; NIST SP 800-26, *Security Self-Assessment Guide For Information Technology Systems*; and NIST SP 800-30, *Risk Management Guide for Information Technology Systems.*

Refer to the *HHS IT Personnel Security Guide* for further guidance.

4.1.2 Rules of Behavior

Procedures

- Establish Rules of Behavior (RoB) for each MA and GSS as a part of the SSP, which should include, but not limited to:

    1. protection of user names and passwords
    2. appropriate use of system resources
    3. virus protection procedures
    4. remote connection
    5. Internet and e-mail use
    6. incident handling
    7. state the consequences of inconsistent behavior or non-compliance.

- Require all users of Departmental systems, including contractors with access to Departmental IT systems, to receive annual training on the RoB for each system to which they will be granted access.
- Ensure users realize that the RoB and associated policies apply even if not thoroughly read through.
- Enforce compliance with RoB by equating any negligence as a security incident, or if deemed willful negligence, a security violation.
- Ensure that users sign the appropriate RoB form(s) included in appendix G.

References

NIST SP 800-26, *Security Self-Assessment Guide For Information Technology Systems.*

For examples of Rules of Behavior, refer to NIST SP 800-18, *Guide for Developing Security Plans for Information Technology Systems*.

Refer to appendix G for the RoB form to sign.

4.1.3 Disciplinary Action

Procedures

- Consult with the Department OHR to establish procedures for disciplinary actions for security violations committed by employees and contractors.

    1. These disciplinary actions should be decided on a case-by-case basis and the sensitivity of information involved and the number of prior offenses should be taken into account.

- Define remedial actions for employees to include the following:

    1. reassignment of work duties

2. disqualification from a particular assignment
3. letter of warning
4. suspension
5. termination
6. removal of contractor staff who commit security violations commensurate with high risk to the Department from the contract.
7. depending on the security violation, criminal sanctions may also apply.

- Report suspected personnel security violations to the OIG for investigation and recommend disciplinary action.
- Specify the disciplinary actions for security violations in security awareness training and the RoB.

References

E.O. 12674, *Standards of Ethical Conduct for Employees of the Executive Branch.*

4.1.4 Acceptable Use

Procedures

- Define, document, and promulgate policies on personal use of Departmental IT resources to all authorized users.
- Inform users that they should not engage under any circumstances in any activity that is illegal under local, state, federal, or international law while using Department-owned resources.
- Inform users that the use of Departmental information resources for anything other than authorized purposes is a violation of the Departmental RoB and could be grounds for disciplinary action.
- Inform users that they are personally responsible for ensuring the use of Departmental workstations and other information resources is solely for officially authorized purposes.
- Inform users that Departmental information resources, including the information within or moving over the systems supported by the Department, are government property.
- Inform users that use of Departmental assets to interfere with or disrupt network users, services, or computers is prohibited; disruptions include, but are not limited to, distribution of unsolicited advertising and propagation of computer viruses.
- Inform users that use of Departmental assets to engage in acts that are deliberately wasteful of computing resources or unfairly monopolize resources to the exclusion of others is prohibited.
-
    1. These acts include, but are not limited to, broadcasting unsolicited mailings or other messages, creating unnecessary output or printing, or creating unnecessary network traffic.

- Inform users that use of Departmental assets that violates the rights of any person or company protected by copyright, trade secret, patent, or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of pirated or other software products that are not appropriately licensed for use by the Department is prohibited.
- Inform users that the use of Departmental assets that reveals an account password to others or allows use of an account by others is prohibited.
- Inform users that use of Departmental assets that violate any policies listed in the Departmental RoB is prohibited.
- Ensure that managers are responsible for oversight of compliance with the code of conduct by the employees or contractors they supervise.
- Inform users that the Department reserves the right to audit networks and systems on a periodic, as-needed basis to ensure compliance with this policy.

References

P.L. 107-347 Title III, FISMA; OMB Circular A-130, Appendix III; FISCAM; NIST SP 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*; NIST SP 800-18, *Guide for Developing Security Plans for Information Technology Systems*; NIST SP 800-26, *Security Self-Assessment Guide For Information Technology Systems.*

4.1.5 Separation of Duties

Procedures

- Establish, document, and enforce procedures to ensure separation of duties for sensitive IT positions.
- Divide mission functions and distinct information system support functions among different individuals and ensure different individuals perform them.
- Review access authorizations periodically to identify functions that should be separated to enhance security.
- Identify duties that should be separated to enhance security (e.g., security personnel who administer access control functions should not be those who administer the audit functions on the information system).
- Require that information system support functions be performed by different individuals (e.g., functions such as system management, system design, application programming, systems programming, quality assurance/testing, library management/change management, computer operations, production control and scheduling, network security, database administration, network administration).
- Establish job rotation cycles based on system criticality and data sensitivity.

References

Refer to the *HHS IT Personnel Security Guide* for further guidance.

4.1.6 Least Privilege

Procedures

- Ensure each user or process is authorized the most restrictive set of privileges or access needed for performing authorized tasks.

References

NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook*, for further guidance.

4.1.7 Security Education and Awareness

Procedures

- Develop, fund, and implement a security education and awareness training program and plan training for all employees involved in managing, using, or operating IT systems.
- Ensure through appropriate contractual provisions, that contractor employees involved in managing, using, or operating IT systems receive security education and awareness training commensurate with their duties.
- Ensure new managers, users, or operators of IT systems receive initial training before being authorized network access and that they receive this training within a maximum of 60 days of appointment.
- Ensure contractors whose primary contractual relationship includes development, installation, management, and/or maintenance of a major application; establish a security training program that includes Rules of Behavior for their staff.
- Provide annual refresher awareness training for all personnel responsible for managing, using, or operating IT systems.

  1. This training may be classroom training or be provided in a form such as e-mail messages, newsletters, memoranda, curriculum materials, or videos.

- Provide training whenever significant changes occur to the office environment or procedures.
- Ensure IT security awareness and training plans reflect the overall and specific security training goals for the year.
- Ensure IT security education and awareness plans contain, at a minimum, the following information:

  1. the training content and subject matter of the IT security awareness and training (e.g., security basics, security planning and management)
  2. the target audience, including Departmental and contractor personnel, for each of the training content areas
  3. the level of training (e.g., awareness or specialized) to be provided for each specific subject matter area and target audience category.

- Ensure IT security training program costs, which refer to all information systems' security education and awareness training costs, include the following:

    1. the amount spent on training products for development or purchase
    2. the amount spent on "managing training," such as scheduling booking, planning, and traveling to attend training
    3. the amount spent on "opportunity costs," such as time spent in training or employee time. (Note: Records of specialized training costs may be found within each Departmental OHR, which are often central repositories of employee training records.)

- Ensure training records include, at a minimum, the number of personnel receiving general security awareness, the number of personnel receiving specialized training, the total number of personnel in the Department, and the total cost of the elements of the IT security training program.
- Conduct security awareness training annually.
- Ensure users have received a copy of or have easy access to: (i) organizational security policies and procedures and (ii) and rules of behavior for the information system or a user manual containing such rules.
- Offer specialized training consistent with NIST SP 800-16 and 800-50 for individuals with specific information system security responsibilities.

    1. Security training must be adjusted to the level of the employee's responsibilities.

- Report summary information on the Department's security education and awareness training program in accordance with instructions contained in the Department's annual data call issued in support of FISMA reporting requirements.

References

Refer to NIST SP 800-16, *Information Technology Security Training Requirements, A Role and Performance Based Model*.

4.1.8 Personnel Separation

Procedures

- Notify all appropriate security personnel of all personnel reassignments, promotions, separations, or retirements.
- Deactivate all accounts within 24 hours of an individual's departure or immediately on those occasions when the terms of departure (including involuntary separation) may cause an immediate security risk.
- Conduct an exit interview to ensure that all access issues are reviewed before an individual departs.

- Transfer all official data and e-mail to the supervisor for review prior to an employee's departure.
- Reformat or otherwise sanitize all IT equipment containing sensitive information before its disposal or reassignment to another employee.
- Require that on the last workday of the employee or contractor, all access devices and credentials be surrendered to the appropriate personnel.

References

P.L. 107-347 Title III, FISMA; OMB Circular A-130, Appendix III.

Refer to the *HHS IT Personnel Security Guide* for further guidance.

See appendix H for a checklist that can be used to support the separation process for Departmental IT staff.

4.2 Physical Access Control

4.2.1 General Physical Access

Procedures

- Control physical access points to sensitive facilities or restricted areas housing information systems that process or display information during working hours, and guard or lock them during non-working hours.
- Verify access authorization before an individual is granted physical access.
- Require that emergency exit and re-entry procedures ensure that only authorized personnel are allowed to re-enter sensitive facilities and restricted/controlled areas containing information systems and system/media libraries after an emergency-related event (e.g., fire drills, evacuations, etc.).
- Establish and maintain an access roster for all limited access rooms or facilities, such as server rooms, network wiring closets, or operations centers at the Department.
- Change combinations or entry codes at least annually or whenever a person who knows the combination departs or no longer requires access or when the combination has been compromised.
- Limit access to individuals who need access through the use of guards, identification badges, or entry devices (e.g., key cards).
- Ensure physical protection measures for areas that house power transformers or distribution panels.
- Safeguard all un-issued keys or other entry devices.
- Review periodically and update the master list of assets in accordance with the configuration management policy.
- Require personnel not on the access roster for a limited access room or facility to sign in and be escorted the entire time present in the room or facility.

  1. The system owner should maintain these sign-in logs for a minimum of

one year.

- Report changes in the status of their systems to the appropriate ISSO.
- Define and record an inventory of the assets to include:

1. **Information Assets.** For example, databases and data files, system documentation, user manuals
2. **Software Assets.** For example, application software, system software, development tools, and utilities
3. **Physical Assets.** For example, computer equipment (processors, monitors, desktop computers, laptops, home systems, firewalls, modems); communications equipment (routers, switches, private branch exchanges [PBX], fax machines
4. **Services Assets.** For example, computing and communications services and general utilities (e.g., heating, lighting, power, and air-conditioning)
5. **Space Assets.** For example, computer rooms, maintenance and workshop areas, power supply areas and general office areas

- Require system owners and contractors operating support systems for the Department to be responsible for ensuring that data processing assets under their control are properly protected through implementing cost-effective physical security measures.

References

NIST SP 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*; NIST SP 800-18, *Guide for Developing Security Plans for Information Technology Systems*; NIST SP 800-26, *Security Self-Assessment Guide For Information Technology Systems.*

Refer to the *HHS IT Physical and Environmental Security Guide* for further guidance.

4.2.2 Physical Security

Procedures

- Inform physical security officials when a system's sensitivity level requires additional protections.
- Alert physical security leadership to locations that house sensitive equipment.
- Report immediately any theft or loss of sensitive equipment to physical security personnel.
- Coordinate with facility management personnel to ensure that appropriate physical security safeguards are allocated to all facilities that contain IT resources.

References

Refer to the *HHS IT Physical and Environmental Security Guide* for further guidance.

4.2.3 Visitor Policy

Procedures

- Ensure visitors, contractors, and maintenance personnel are authenticated through the use of preplanned appointments and identification checks.
- Ensure visitors, contractors, and maintenance personnel are formally signed in, escorted, and activities monitored when required.
- Maintain visitor logs that include: (i) the name; (ii) date; (iii) time of entry; (iv) time of departures; (v) purpose of visit; and (vi) person(s) visited
- Ensure visitor logs are closed out at the end of each month and reviewed by appropriate organization officials.
- Maintain and routinely review visitor logs for a minimum of one year.

References

Refer to the *HHS IT Physical and Environmental Security Guide* for further guidance.

4.3 Environmental Security

Procedures

- Maintain sufficient measures for protecting IT systems against environmental factors (e.g., dust, power, excessive heat and humidity). Specialized equipment and devices to monitor and control the environment should be installed. These controls should include:

  1. positioning sensitive IT systems and equipment on raised floors
  2. equipping under-floor areas in all data and operations centers with water detectors
  3. testing controls protecting the environment (power, temperature, fire protection, lighting, plumbing) against disruptions and natural disasters at least annually.

- Monitor environmental conditions for conditions that could adversely affect the operation of sensitive IT systems and information processing facilities.
- Ensure awareness training for system owners, system administrators, and other appropriate staff that covers the procedures to follow during and after an environmental event in areas containing IT systems under their control.

  1. This training should include identifying the location of shutoff valves in proximity to IT systems and evacuation plans.

References

NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook*, for further guidance.

4.3.1 Fire Prevention

Procedures

- Maintain smoke and thermal detectors, and fire suppression equipment in all data and operations centers and within close proximity of primary IT systems.
- Install a fully automatic fire suppression system (compliant with GSA requirements and guidelines) that automatically activates when it detects heat or smoke particles in order to prevent danger to personnel from toxicity.
- Check fire suppression and prevention devices and systems periodically, such as potential failures of electronic devices or wiring, improper storage of materials and promptly resolve all deficiencies.
- Maintain smoke and thermal detectors and fire suppression equipment in all data and operations centers and within close proximity of primary IT systems.
- Equip under-floor areas in all data and operations centers with smoke and water detectors.
- Store hazardous or combustible materials securely at a safe distance from all IT systems.
- Ensure that all fire doors within close proximity of IT systems are alarmed and slam shut.
- Ensure physical barriers are, if necessary, extended from real floor to real ceiling to prevent environmental contamination, such as that caused by fire and flooding.
- Ensure all appropriate staff receives awareness training in fire safety, testing fire alarms, and evacuation plans for areas containing IT systems under their control.

References

NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook*; NIST 800-18, *Guide for Developing Security Plans for Information Technology Systems;* NIST 800-34, *IT Contingency Planning Guidelines*; GAO *Federal Information System Controls Audit Manual* (FISCAM).

Refer to the *HHS IT Physical and Environmental Security Guide* for further guidance.

4.3.2 Supporting Utilities

Procedures

- Review utilities, such as air conditioning, regularly to ensure operability.

- Ensure an uninterruptible power supply (UPS) and/or backup generator is provided so that critical operations may continue and to prevent system crashes as a result of power failure.

- Ensure all critical servers, computers, and IT equipment are connected to power strips or surge suppressors.
- Ensure an automatic emergency lighting system is installed to cover all areas necessary to maintain mission or business essential functions, including emergency exits and evacuation routes.
- Ensure a master power switch or emergency cutoff switch to sensitive IT equipment is present. The cutoff switch shall be located near the main entrance of the sensitive area and shall be labeled and protected by a cover to prevent accidental shutoff.
- Ensure building plumbing lines are NOT endangering the computer/server room or any room that contains sensitive equipment. At a minimum, shutoff-valves and procedures shall exist and are known by staff members.
- Ensure that plastic sheets are readily available in the computer/server room or in any room that contains critical equipment to protect them from accidental water leaks from building plumbing lines or in the event the sprinkler system malfunction.

References

FIPS 31, *Guidelines for Automatic Data Processing Physical Security and Risk Management;* NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook*; NIST SP 800-18, *Guide for Developing Security Plans for Information Technology Systems;* NIST 800-34, *IT Contingency Planning Guidelines;* GAO *Federal Information System Controls Audit Manual* (FISCAM).

Refer to the *HHS IT Physical and Environmental Security Guide* for further guidance.

4.4 Media Control

4.4.1 Media Protection

Procedures

- Establish Department-wide procedures for access, storage, and transportation of all media containing sensitive information.

  1. These procedures should include logs to track deposits and withdrawals of media from on-site storage facilities, libraries and backup storage facilities, and procedures for the proper wrapping and labeling of media to be mailed or couriered.

- Maintain an accurate Department-wide record of the media’s chain of custody and hold users accountable for the media removed from storage.
- Label and keep all media in a secure location on site.

1. Backup and archive media should be sent to a secure off-site location, as identified by the Departmental business continuity and disaster recovery plans.

- Monitor sensitive information in the following ways:

  1. Do not leave sensitive information unattended, even temporarily.
  2. Keep sensitive material in a secure, safe or locked cabinet and return all sensitive information to that location at the end of each business day.
  3. Provide physical and environmental protection controls for sensitive data contained in a media storage vault or library.
  4. Turn over, place out of sight, or remove from the screen sensitive information when visitors are present.
  5. Sanitize or destroy diskettes and other magnetic storage media that contain sensitive data when they are no longer needed to store the sensitive data.

- Establish records to track all deposits and withdrawals from media storage facilities and libraries.

  1. Secure records from unauthorized access to prevent unauthorized access and manipulation of log information.
  2. Maintain records of the delivery and receipt Department-wide for media that are transferred to another location by courier or mail.

- Dispose of both electronic and hard copy media in accordance with the Departmental sanitation and disposal policy.

References

P.L. 107-347 Title III, FISMA; OMB Circular A-130, Appendix III.

Refer to the *HHS Contingency Planning for Information Security Guide* for further guidance.

4.4.2 Media Marking

Procedures

- Label media with the appropriate sensitivity level for the information stored on the media; sensitive data shall be dated and marked as such.
- Ensure appropriate security labels that reflect the distribution limitations and handling caveats of the information are affixed to all information system output.
- Ensure removable information storage media contain external labels indicating the distribution limitations and handling caveats of the information.
- Mark removable magnetic media so it can be distinguished from other types of media.
- Ensure all Departmental media are marked “For Official Use Only.”

- Label and store backup media used for disaster recovery, off-site in a designated location.

References

NIST SP 800-18, *Guide for Developing Security Plans for Information Technology Systems*; NIST SP 800-26, *Security Self-Assessment Guide For Information Technology Systems.*

4.4.3 Sanitization and Disposal of Information

Procedures

- Dispose of retired, damaged, discarded, or unneeded information in a manner that prevents unauthorized persons from using it.
- Sanitize and destroy media in accordance with the Departmental sanitation and disposal policy.
- Ensure that information is never disclosed during disposal unless authorized by statute.

  1. Cleared or sanitized media that previously contained information at a designated FIPS Publication 199 security category (for confidentiality) is reused at the same or higher security category.
  2. Sanitized media is downgraded only with appropriate approval(s).

- Destroy hard copy documents when no longer needed with methods for destroying organizational information in paper form including: (i) burning—the material is burned in either an incinerator that produces enough heat to burn the entire bundle or the bundle is separated to ensure all pages are consumed; (ii) mulching or pulping—all material is reduced to particles one inch or smaller; (iii) shredding or disintegrating—paper is shredded in cross-cut shredders (preferred) or strip shredders (alternative).

  1. Information storage media is destroyed in accordance with organization-approved methods.
  2. An authorized contractor accomplishes document destruction in the absence of the organization's direct participation.

- Ensure equipment removal procedures for information systems and components that have processed or contained organizational information are followed, which may include inspection of the information system by designated individuals to ensure that all media, including internal disks, have been removed or sanitized.
- Ensure that only approved equipment or software is used to degauss or overwrite magnetic media containing organizational information.

  1. Each action or procedure taken to overwrite or degauss such media is verified.

- Ensure all memory locations are overwritten three times (the first time with a random character, the second time with a specified character, and the third time with the complement of that specified character) to clear all magnetic media (i.e. diskettes, floppy disks, etc.).

    1. The success of the overwrite procedure is verified through random sampling of the overwritten media.
    2. Items that have been cleared (i.e., not sanitized) remain at the previously designated FIPS Publication 199 security category (for confidentiality) and remain in a secure, controlled environment.

- Ensure data stored on electronic media (e.g. optical media, CD-Rs, hard drives) is permanently deleted and unrecoverable before media is disposed of or identified as surplus.
- Sanitize all IT systems storage media containing sensitive information, including clearing, purging, and destroying.
- Sanitize magnetic media, diskettes, hard disks, or other storage devices containing sensitive data or software prior to transferring, reusing, or donating any equipment or media.
- Overwrite or degauss removable or portable media that is to be reused.
- Require a contract with any contractor to prevent the disclosure of sensitive information on systems, hard drives, or media sent outside of the Department for repair or data recovery.

References

FISCAM; NIST SP 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*; NIST SP 800-18, *Guide for Developing Security Plans for Information Technology Systems*; NIST SP 800-26, *Security Self-Assessment Guide For Information Technology Systems*; NIST SP 800-30, *Risk Management Guide for Information Technology Systems.*

See appendix I for a Cleaning and Sanitization Matrix and appendix J for a Media Disposal checklist.

4.4.4 Input/Output Controls

Procedures

- Establish procedures to ensure media, including tapes, disks, and paper, are neither accessed nor stolen by unauthorized individuals, which may include:

    1. Obtain locked or secured physical bins to place printouts from high-speed printers and from facsimile (fax) machines.
    2. Enable banner settings for all print jobs.
    3. Use certified mail when mailing sensitive information.

    4. Require users to be present at the printer when they print

sensitive information.

References

Refer to the *HHS IT Physical and Environmental Security Guide* for further guidance.

4.5 Data Integrity

Procedures

- Implement data integrity controls and include procedures for maintaining such controls in the SSP.
- Review audit logs periodically to determine integrity of system data.
- Documentation procedures include:

- Maintain logs for system documentation.
- Ensure that adequate documentation is maintained that explains how software, hardware, and IT systems are to be used, and that formalizes security and operational procedures specific to the Department-wide systems.
- Ensure that networks and systems diagrams are developed to illustrate the interconnection of system components, their locations, and data flow.
- Ensure that system owners develop a SSP for each MA and GSS under their control and responsibilities.
- Typical security documentation that support the security of MAs and GSSs and the C&A process is listed below. This list is not intended to be all-inclusive or to imply that all systems should have all the items listed.

  a. Vendor-supplied documentation of software and hardware
  b. Applications and/or systems requirements
  c. Application and/or system security plans
  d. Application program documentation and specifications
  e. Security Test and Evaluation (ST&E) plan and procedures
  f. Standard Operating Procedures
  g. Contingency plans (i.e., emergency, incident response, disaster recovery, backup procedures)
  h. MOAs or MOUs with interfacing systems
  i. System rules of behavior
  j. Security awareness and training
  k. User manuals
  l. Risk assessments/security self-assessments
  m. Security Requirements Traceability Matrix (SRTM) or Baseline Security Requirements (BLSR)
  n. Plan of Action and Milestones (POA&M)
  o. Authorization processing/accreditation documents and statements (i.e., security certification and security accreditation)

References

NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook*, for further guidance; NIST SP 800-18, *Guide for Developing Security Plans for Information Technology Systems*; NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*.

4.6 Communications Security

4.6.1 Voice Communications

Procedures

- Restrict access to PBX equipment to only authorized personnel.
- Disable (if possible) or monitor remote access ports.
- Ensure minimum requirements for the physical protection of digital switches and key system facilities such as locks, access logs, and escort procedures.
- Avoid co-locating the PBX system(s), voice mail system(s), and their administrative terminals with other equipment requiring human access.

1. If space allows, consider locating the switch terminals in separate rooms.
2. Use locks and alarms to control access to the equipment.

References

NIST Special Publication 800-24, *PBX Vulnerability Analysis: Finding Holes in Your PBX Before Someone Else Does;* and NIST SP 800-13, *Telecommunications Security Guidelines for Telecommunications Management Network.*

4.6.2 Data Communications

Procedures

- Place fax servers and gateways that connect a Departmental Internet Protocol (IP) network to an external IP network (e.g., the Internet) on extranets
- Ensure fax modems and boards are not directly attached to networked workstations. Fax modems and boards may be directly attached to stand-alone workstations.
- Encrypt sensitive information during receipt, transmission, and storage using a method compliant with FIPS.
- Implement role-based access control mechanisms (e.g., password protected in box) onto fax servers and gateways that store sensitive data.
- Disable and enable authorized remote maintenance (e.g., dial-in) ports for fax servers, gateways, and other systems only as needed for authorized maintenance or repair.
- Scan all received binary files using fax protocols with virus-checking software.
- Implement encryption at the data link level, transport level, or application level.

References

Federal Information Processing Standards (FIPS) 140-2 or FIPS 197 Advanced Encryption Standard (AES).

Refer to the *HHS Data Cryptography Guide* for further guidance.

4.6.3 Video Teleconferencing

Procedures

- Ensure that adequate security controls are implemented to ensure that only authorized individuals can participate in video teleconferencing.
- Ensure that transmission protection is commensurate with the highest sensitivity of information to be discussed over the video teleconference.
- Ensure that video teleconferencing equipment and software are turned off when not in use.

References

National Communications System (NCS) Federal Telecommunications Recommendation (FTR), *Video Teleconferencing Services at 56 to 1,920 kbit/s.*

4.6.4 Voice-Over Internet Protocol

Procedures

- Appropriately configure computer operating systems when used for Voice-Over Internet Protocol (VoIP) transmissions to preserve security protections.
- Ensure shared media devices (e.g., hubs) are not installed on VoIP networks.
- Configure VoIP networks to function as an alternate telephone service if major network problems occur.
- Configure all Departmental firewalls properly to recognize authorized VoIP networks and systems.

References

NIST DRAFT SP 800-58, *Security Considerations for Voice Over IP Systems.*

4.6.5 Facsimile

Procedures

- Ensure operation and usage follow the procedures below.

1. Ensure that accurate phone numbers are used for fax transmissions and ensure that broadcast lists used to automate the sending faxes are accurately maintained.
2. Ensure that sensitive information is not sent by fax on an unencrypted line.
3. Monitor or use password-protected in boxes for received data during operational hours on stand-alone fax machines that are used for receiving sensitive data.

    a. Management may choose to waive this requirement if an operating environment has sufficient physical access controls to prevent unauthorized access to sensitive fax output.

- Ensure binary files received using fax protocols are scanned using virus-scanning software.
- Ensure the encryption of sensitive information during receipt/transmission using a FIPS 140-2 compliant method.

    1. Encryption can be implemented at the data-link level, transport level, or application level.

References

P.L. 107-347 Title III, FISMA; OMB Circular A-130, Appendix III; *Privacy Act of 1974*; FIPS 140-2, *Security requirements for Cryptographic Modules*; NIST SP 800-13, *Telecommunications Security Guidelines for Telecommunications Management Network.*

4.7 Wireless Communications Security

4.7.1 Wireless Local Area Network (WLAN)

Procedures

- Ensure that WLAN infrastructures are deployed under the utmost security and provide wireless plan to OPDIV CISOs for approval.
- Ensure unsecured WLANs are not used to transmit sensitive or privacy-related data.
- Separate WLAN infrastructure from the wired LAN infrastructure with a NIST-approved firewall.
- Ensure OPDIV CISOs who authorize WLANs establish monthly vulnerability testing to ensure WLAN security, including scanning for rogue access points.
- Ensure OPDIV CISOs conduct monthly sweeps of Departmental business locations to locate and disable unauthorized wireless access points.
- Ensure that DAA approves the implementation and use of WLANs at a specified risk level prior to operation.

References

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

Refer to the *HHS Wireless Security Guide* for further guidance on using wireless communications.

4.7.2 Multifunctional Wireless Devices

Procedures

- Conduct a risk assessment on all wireless devices

  1. Risk assessments should include the risks associated with all functions, including infrared, radio frequency (RF), and video transmissions.
  2. The DAA should analyze the associated risks identified by the risk assessment and develop guidelines for their applicability and use, based on the sensitivity of the data involved and the acceptability of identified risks.

- Develop procedures for removing data from multifunctional wireless devices before transferring or disposing of the equipment.

References

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

Refer to the *HHS Wireless Security Guide* for further guidance.

4.8 Equipment Security

4.8.1 Workstations

Procedures

- Use only licensed and approved operating systems and applications on Departmental desktop computers or workstations.
- Ensure that all Department-owned workstations have an asset tag and are inventoried with name, location, and use.
- Change all default vendor or manufacturer-set administrator accounts and passwords before installation or use.
- Ensure that all workstations are equipped with the standard HHS-approved antivirus software and configured to automatically perform periodic virus scanning.

References

NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook*, for further guidance.

4.8.2 Laptop Computers and Portable Computing Devices

Procedures

- Ensure that all Department-owned laptops and Portable Computing Devices (PCDs) are controlled using Departmental accountability procedures, such as having asset tags and being inventoried with name, location, and use.
- Ensure that all laptop cases are marked with an asset tag or engraved with the Department address and a phone number.
- Based on sensitivity, new laptops should be equipped with "dial home" software that can be used to communicate with the Department and assist police in recovering stolen equipment when it is technically and financially feasible.
- Equip all new laptops to support file encryption.
- Require all users to report immediately any incidents of mishandling or loss of a laptop computer or PCD to the applicable Departmental security office.
- Ensure that all Basic Input/Output Systems (BIOS) and sensitive files on the laptop hard drive are password protected.
- Store laptops and PCDs in a lockable cabinet when not in use, and do not leave laptops or PCDs unattended.
- Ensure that all laptops and PCDs used for Department business, whether personally- or government-owned, employ antivirus software and users maintain current virus signature files.
- Back up critical data before going on travel.
- Ensure property inventory lists to include the serial numbers and/or seat numbers, user names, and location of laptops and PCDs.

  1. Users are directly accountable for their laptop computers and PCDs.
  2. Users should sign a receipt assuming responsibility for the laptop computer or PCD by serial number.
  3. Users are restricted to individuals that sign the receipt without registering a formal change of accountability.

- Require users of laptops/PCDs that process sensitive information to sign a responsibility statement that stipulates their understanding of the necessary security measures and policies governing the use of the laptop computers/PCDs.
- Ensure, before disposal, that all laptop computers/PCDs that processed sensitive information are cleaned by commercial disk-wiping software and have had the hard drives and memory chips degaussed.

1. The individual(s) performing these activities must sign a letter stipulating compliance with all disposal security requirements; this letter must accompany any IT equipment turned into property management for disposal.

References

FIPS 31, *Guidelines for Automatic Data Processing Physical Security and Risk Management.*

4.8.3 Personally Owned Equipment and Software

Procedures

- Provide all Departmental employees and contractors with security awareness training on prohibitions against the use of personally owned equipment and software for official business.
- Conduct reviews, at least semiannually, of all equipment and software in Departmental offices to ensure that only government-licensed software and equipment is used to conduct official business.
- Require appropriate waivers to be signed by the DAA for personally owned equipment or software in use in the Departmental offices or connected to Departmental networks and/or systems remotely.

References

FIPS 31, *Guidelines for Automatic Data Processing Physical Security and Risk Management.*

4.8.4 Hardware Security

Procedures

- Ensure only authorized IT practitioners (e.g., system administrators, vendor technicians) perform maintenance activities on hardware or software, and visiting practitioners should adhere to sensitive facility policy.
- Ensure contracts with maintenance vendors identify the security requirements.
- Log changes made to hardware or software during maintenance.
- Ensure, following IT system upgrades or consolidations, that surplus equipment is secured, locked up, and managed by the OPDIV ISSO until it has been prepared for surplus.
- Prevent potential hardware disruptions by conducting routine hardware inspections to mitigate sources of potential disruption and repair as appropriate.
- Ensure all repairs and/or maintenance activities are approved by the appropriate systems owner prior to implementation, as required.

1. Coordinate system repairs and/or maintenance with the appropriate systems owner and users to reduce potential disruptions to workflow and support to essential functions.
2. Conduct hardware maintenance during non-business hours, when possible, to reduce potential disruptions to normal operations.
3. Conduct data backup prior to system repair and/or maintenance, if possible.

References

FIPS 31, *Guidelines for Automatic Data Processing Physical Security and Risk Management.*

Refer to the *HHS Configuration Management Guide* for further guidance.

4.8.5 Software Security

Procedures

- Ensure all repairs and/or maintenance activities are approved by the appropriate system owners prior to implementation and meet common criteria requirements, as required.
- Coordinate software maintenance activities with the appropriate system owners and users to reduce potential disruptions to workflow and support to the Department's essential functions.

    1. Conduct software maintenance during non-business hours, when possible, to reduce potential disruptions to normal operations.
    2. Conduct system file and data backup prior to conducting software maintenance, if possible.

- Install applicable software patches and assure that new software patches are promptly installed.

References

FIPS 31, *Guidelines for Automatic Data Processing Physical Security and Risk Management.*

Refer to the *HHS Configuration Management Guide* for further guidance.

4.8.6 Hardware and Software Maintenance

Procedures

- Conduct comprehensive maintenance testing that systematically schedules information system hardware for periodic maintenance inspections and testing to ensure the equipment operates within design specifications and is properly calibrated.

- Conduct routine periodic hardware preventive maintenance in accordance with vendor specifications and in a manner that minimizes the impact on operations.
- Document all the repairs and modifications of the physical components of a facility that are related to security (e.g., hardware, walls, doors, and locks).
- Ensure regular and unscheduled hardware maintenance performed is also documented, to include:

  1. the date and time of maintenance
  2. name of the individual performing the maintenance
  3. name of escort
  4. a description of the type of maintenance performed, to include identification of replacement parts

- Sanitize or appropriately clear any component of information systems or system components containing nonvolatile memory that is to be removed from the facility for repair, with its release explicitly approved by an appropriate organization official.
- Conduct a configuration management review of maintenance changes that impact the security of the information system.
- Check system features to assure that they are still functioning properly after maintenance is performed on the information system.
- Conduct maintenance in a manner that maintains security.

References

NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook*, for further guidance.

4.9 Contingency Planning

Procedures

- Develop a contingency plan for the information system that is compliant with OMB policy and consistent with the guidance provided in NIST SP 800-34.
- Ensure the approval of the contingency plan by key affected parties.
- Review the plan once a year, reassess, test and, if appropriate, revise to reflect changes in hardware, software and personnel.

References

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

4.9.1 Security Incident and Violation Handling

Procedures

- Develop an incident-response plan consistent with NIST SP 800-61 that defines reportable incidents and events, outlines a standard operating procedure for incident response (to include actions to protect evidence in support of forensics), provides for user training, and establishes an incident-response team.

  1. An incident is defined as: the violation, or an imminent threat of a violation, of an explicit or implied security policy, acceptable use policies, or standard security practices in a computing or telecommunications system or network. While certain adverse events, (e.g., floods, fires, electrical outages, and excessive heat) can cause system crashes, they are not considered computer-security incidents.
  2. An event is defined as: an observable occurrence in a network or system.

- Test the incident-response plan at least annually with test results used to modify the incident-response plan as necessary to ensure effectiveness.
- Ensure reports of possible security violations and security incidents are accurate and timely.
- Define appropriate parameters for the response of security incidents, which may include: (i) what information employees must provide; (ii) whom they must notify; and (iii) what degree of urgency to place on reporting.
- Review intrusion-detection reports and handle suspected incidents accordingly.
- Review records of information system activity, such as security incident tracking reports.
- Investigate security violations, security incidents, and suspicious activities (e.g., failed logon attempts, other failed access attempts; and questionable activity) and report results appropriately.
- Maintain the Secure One Communications Center (SOCC) as a mechanism for receiving and disseminating computer security incident information throughout the Department.

  1. Inherent in the SOCC operation is the capability to respond to and report on computer security incidents.
  2. The SOCC functions in accordance with federal policy and regulations including OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources;* Presidential Decision Directive (PDD) 63: *Critical Infrastructure Protection*; and *FISMA*.
  3. The SOCC also provides the Department with the following:

     a. framework for identifying, handling, managing, responding to, and reporting computer incidents timely and expeditiously
     b. government-wide information sharing of threats, incidents, and trends to support computer security planning and operations.

4. Upon identification of an incident, the appropriate Incident Response Team (IRT) must contact the SOCC within two hours to report basic information about the incident (e.g., what happened, what is the initial damage. Within four hours of the initial report, the IRT must provide further details of the incident by using the Incident Reporting Survey in the ISDM or by telephone or email.
5. IRTs should use the following priority levels, based on Federal Computer Incident Response Center's (FedCIRC) priority levels, to further define the incident:

    a. Priority Level 1—possible life-threatening activity, or affects classified or critical systems or information.
    b. Priority Level 2—could become public; provide successful or unsuccessful unauthorized access to a network and/or unclassified, non-critical information; affect system resources; or shows active targeting of a classified/critical system.

- Categorize all incidents and events when reporting them to the SOCC by using the following categories:

Note: The incident categories listed below are neither comprehensive nor intended to provide definitive classification for incidents; rather, they simply give a basis for providing a list of certain types of incidents. Also, some incidents may fit into more than one category.

1. malicious code: a virus, worm, Trojan horse, or other code-based entity that is either successful or unsuccessful in infecting a host. This category applies to incidents and events.
2. probes and reconnaissance scans: involve searching the network for critical services or security weaknesses.
3. inappropriate usage: a person violates acceptable computing use policies, such as sending spam, email threats, or making illegal copies of software.
4. unauthorized access: a person gains logical or physical unauthorized access to a network, system, application, data, or other resource. This access may include root compromises, unauthorized data alterations, Web site defacements, loss/theft of equipment, unauthorized use of passwords, and use of packet sniffers.
5. denial of service (DoS) attacks: a successful or unsuccessful attack (including Distributed Denial of Service Attacks) impairs the authorized use of networks, systems, or applications by exhausting resources, to include Distributed DoS attacks.
6. other types of incidents include, but are not limited to:

    a. alterations/compromises of information
    b. adverse site mission impacts
    c. classified system incidents
    d. loss or theft of equipment.

- Provide the following information when reporting an incident to SOCC:

  1. point of contact (POC) information (name, email address, title, telephone number, OPDIV)
  2. support action requested and the timeframe
  3. entities with which SOCC and FedCIRC can share incident data
  4. approximate start time of incident and current status
  5. information on the attacking computer(s) and victim computer(s)
  6. targeted operating system
  7. ports targeted in attack
  8. primary purpose of the targets/victims involved
  9. number of hosts affected.

- Report adverse events that are not usually within the scope of computer security incident response, which include unplanned outages and acts of nature such as floods and fires.

  1. The Department should report these types of incidents within a two-hour time frame.
  2. The Department should address these types of incidents in the component's business continuity procedures or contingency plans.

- Report the incident once it is determined that a significant computer security incident exists, and perform "triage" as necessary.
- Ensure all parties work to preserve evidence of computer crimes.

  1. Document and retain notes, save and back up all incident-related logs, and maintain a chain of custody log as part of investigations
  2. Gather evidence, including all appropriate audit files and logs, and preserve where feasible.

- Perform an initial assessment and investigation to determine the existence of a computer security incident.
- Provide sensitive incident reports through any official mode of communication (e.g., fax machines, e-mail, or telephones) appropriate to the sensitivity level of the report.

  1. Follow-up reports based on the type and severity of the incident may be requested.
  2. Computer security incident reports are not releasable under *Freedom of Information Act (FOIA) Exemption (b).*

- Evaluate each incident to determine reporting requirements to external law enforcement agencies or other organizations, as applicable.
- Coordinate with all external incident response organizations such as the FedCIRC, Carnegie Mellon's Computer Emergency Response Team (CERT), the National Security Incident Response Center (NSIRC), and the National Infrastructure Protection Center (NIPC).

- Report incident trends to the HHS CIO and other senior Departmental management, as warranted, based on the significance of the trend.
- Establish a primary point of contact and key staff to assist in a response process for all handling and reporting incidents.
- Train staff on the appropriate incident response handling procedures.
- Use available tools, such as intrusion detection and security monitoring software, to aid staff in obtaining early warning of possible incidents.
- Modify incident handling procedures and control techniques after an incident occurs, as required.
- Ensure that information on common vulnerabilities and threats is shared with system owners of interconnected systems.

References

P.L. 107-347 Title III, FISMA; NIST SP 800-61, *Computer Security Incident Handling Guide*; *Computer Fraud and Abuse Act 1986.*

Refer to the *HHS Incident Response Planning Guide* for further guidance.

4.9.2 IT Disaster Recovery and Continuity of Operations

Procedures

- Ensure provision for temporary emergency operation of critical systems and for restoring normal operation of systems after a catastrophic event.
- Ensure the effective continuation of core services and processes required to accomplish the Departmental mission during and after a disaster.
- Ensure the restoration of all core services and processes after a failure, no matter the cause.
- Account for the four elements in a Business Continuity Plan (BCP)/Disaster Recovery Plan (DRP) to assure continuity planning activities:

    1. **Participants.** This element evaluates the human impact of a disaster on core services' employees and their families and core services' customers and suppliers. Each potential participant may have very different needs after a disaster than before a disaster.
    2. **Processes.** This element assesses the vulnerability of routine core services' business practices to a disaster. This assessment accounts for disruptions in strategy (e.g., failure of parts of the core services business model); finances (e.g., inability to pay employees or buy equipment from suppliers); operations (e.g., inability of core services to carry out some or all of its mission); and relationships (e.g., problems with civil authorities, third-party service providers, or insurance companies).

3. **Infrastructure and Resources.** This element examines how a disaster affects the core services' physical plant including, but not limited to, equipment, software, buildings, electrical power, backup tapes, and transmission facilities. It addresses such items as restoration priorities, damage assessments, salvage, and in turn develops methods to obtain required equipment or services.
4. **External Dependencies.** This element takes into account the dependencies that core services have on other services that are not under its direct control. These might include base security, fire/rescue, water/sewer, hospitals, transportation, food, etc.

- Ensure BCP/DRP services planning encompasses the following:

1. Identification of Departmental functions

    a. A recovery time objective (RTO) should be established for each function. The RTO is the longest time period in which a function can be disrupted before the disruption causes serious harm to the organization. During an emergency, essential government functions should be recovered and reconstituted no later than the RTO; recovery of other functions deemed non-critical should be deferred.

2. Develop a recovery strategy and procedures for resuming each essential Departmental function, including the associated system, data, application, and telecommunications.

    a. The procedures should include instructions for backing up and restoring tasks, a method for reconstructing lost data, steps for implementing alternative work methods or emergency operations, steps required for managing and processing work backlog, and a procedure to synchronize files and data. The recovery strategy should be assessed for sufficiency in meeting the recovery time objective for the essential Departmental function. The Department should acknowledge risk and any associated data loss.

3. Mitigate service degradation that may be caused by implementing recovery strategies.

    a. Strategies may make use of internal recovery, commercial recovery centers, or cooperative agreements or may involve a combination of the aforementioned. Implementing the strategy may be achieved via hot sites, cold sites, mutual-internal support, or reciprocal agreements.

4. Develop a schedule for ramping up or rapidly resuming each essential Departmental function.

- Establish and maintain a vital records program.

1. Vital records should be identified, duplicated, and stored off premise in a suitable environment located a safe distance from the Department.

- Provide guidance for performing physical and information security.
- Conduct a business impact analysis (BIA) to determine the prioritization of recovering mission-critical systems, where appropriate.
- Establish and maintain system-specific Disaster Recovery and Continuity of Operations Plans.
- Perform BCPs/DRPs using a planning cycle that includes the following phases:

  1. defining functional requirements (including risk assessment and BIA activities)
  2. baselining current recovery capabilities
  3. designing and developing response and recovery strategies
  4. developing the BCP/DRP
  5. implementing the plan (including corporate awareness and education programs)
  6. maintaining the plan and the associated emergency response capability.

- Develop a plan using an integrated planning approach, which involves:

  1. a team composed of individuals with expertise in Departmental business operations, IT (voice and data), security, business continuity/disaster recovery, and facilities
  2. a coordinated approach with other federal, state, and local governments and with private sector organizations when necessary

     a. This approach not only ensures that all plans, infrastructures, and capabilities are interoperable but also mitigates conflicting lines of authority.

  3. a strategy and procedures for responding to emergencies (including building evacuation), relocating to one or more alternate operating facilities, restoring utility (voice and data), restoring operations and processing any backlog of work, resuming essential government functions, moving to any interim operating site(s) during the recovery period, and returning to the home site.

- Promote a general understanding of BCP, disaster recovery planning, and IT contingency planning concepts throughout the Department.
- Designate emergency staff (teams), duties and responsibilities, and procedures for notification and recall of the emergency staff (teams) during duty and off-duty hours.
- Identify preventive controls and practices that can reduce the effects of system disruptions, reduce the costs associated with recovery, and increase system availability, where appropriate.

References

P.L. 107-347 Title III, FISMA; OMB Circular A-130, Appendix III; NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems.*

Refer to the *HHS Contingency Planning for Information Security Guide* for further guidance.

4.9.3 Backup Data

Procedures

- Document and implement proper backup procedures for each IT system, including:

  1. frequency of backups
  2. duration for retaining backup archives
  3. rules for archiving backups, including instructions on off-site storage
  4. off-site schedules, including lists of personnel authorized to handle and process backup media
  5. logs of backups, including recording errors that may have occurred.

- Develop procedures to test backup via restoration of information from backup media.
- Rotate backup files off site at a frequency appropriate for the system to avoid disruption if current files are damaged.
- Perform checks and assign responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.
- Consider using technical features that enhance information integrity and availability including, among others, remote journaling, Redundant Array of Inexpensive Disks (RAID), and similar techniques.
- Ensure all Departmental data storage facilities are configured to respond to FOIA inquiries, requests from Congress, official government investigations, and authorized requests stemming from litigation.
- Protect backups at the highest level of sensitivity and marked appropriately.
- Restrict backups to authorized personnel only.
- Perform verification tests on all backups at least once per month.

References

OMB Circular A-130, Appendix III; NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems.*

Refer to the *HHS Contingency Planning for Information Security Guide* for further guidance.

4.9.4 Store Backup Data

Procedures

- Ensure that the backup storage location is:

  1. a safe distance from the primary system and the operation/data center
  2. independent of the environmental conditions of the primary system location and operation/data center (e.g., threat of flood or earthquake)
  3. not impacted by the same disruptions as the primary system location and operation/data center (e.g., electrical outages).

- Store backup copies of the operating system and other critical software in a fire-rated container that is not collocated with the operational software.

References

NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems*, for further guidance.

5. Technical Controls

5.1 Identification and Authentication

Procedures

- Implement Identification and Authentication (I&A) mechanisms, including provisions for uniquely identifying and authenticating entities (i.e., users or information system processes acting on behalf of users).
- Require access to an information system be gained through the presentation of an individual identifier (e.g., a unique token or user login identification [ID]) and authenticator(s).
- Explicitly identify any user actions that can be performed prior to reliable identification (e.g., reading a publicly available Web site).
- Ensure the basis of identification and authentication is on one of the three principles of I&A:

  1. what one knows (e.g., passwords)
  2. who one is (e.g., fingerprint, retinal pattern)
  3. what one possesses (e.g., token, cryptography key).

References

FIPS 186-2, *Digital Signature Standard*; NIST SP 800-18, *Guide for Developing Security Plans for Information Technology Systems.*

5.1.1 Identification

Procedures

- All users must have their identity verified to each IT system with a unique user-ID and associated password prior to being permitted to use IT systems connected to the HHS network. This identification is performed each time the password is required.

  1. Ensure that each individual applies for and uses only one user-ID during his/her tenure as a Departmental employee or contractor.
  2. Revoke assigned user-IDs upon termination of employment.

- Do not reissue a user-ID to another person for one year after its previous deletion.
- Ensure users, system administrators, and security persons who require “super/administrator privileges” use their individual user-ID to gain access to restricted functions (e.g., root access).
- Deny the use of shared accounts.

References

NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook*, for further guidance.

5.1.2 Authentication

Procedures

- All users shall use one or more authentication methods: password, biometric, or token.

5.1.2.1 Password

Procedures

- Ensure passwords are not shared, displayed online, made visible at session initiation or divulged publicly.
- Ensure passwords are a minimum of eight characters.
- Ensure passwords are non-words, mixing letters and numbers.

1. at least one uppercase letter, one lower case letter, and one number are required, and no words found in a dictionary will be allowed.

- Ensure passwords are not sports names, pet names, family names, employee name, or user Ids.
- Ensure passwords automatically expire every 90 days, with the security software prompting each user for a new password daily beginning 14 days prior to the expiration date.
- The password expiration is a risk based management decision and OPDIVs are encouraged to require a shorter time period for password expiration for more sensitive information systems.
- Ensure passwords are not reused until at least six other passwords have been used.

5.1.2.2 Biometric Controls

- Biometric controls can be used in addition to or instead of a password.

a. These controls can include retinal scans, fingerprint scans, etc.
b. The level at which biometric controls will be required is dependent on HHS and OPDIV needs and feasibility.

5.1.2.3 Token

- Tokens can be used in addition to a password or biometric.
- Four types of tokens are acceptable: hard tokens, soft tokens, one-time password devices, and password tokens.

1. Hard Token

   a. Ensure that a password or biometric is used to activate an authentication key.
   b. Ensure that authentication keys are not exportable
   c. Ensure that any hard token that is used is FIPS 140-2 validated.

2. Soft Tokens

   a. Ensure that the activation data will be a password known only to the user
   b. Ensure that the cryptographic module shall be FIPS 140-2 validated
   c. Ensure that the unencrypted copy of the authentication key shall be erased after each authentication.

3. One-Time Password Device Token

   a. The device may or may not have some kind of integral entry pad, an integral biometric (e.g., fingerprint) reader or a direct computer interface (e.g., USB port).
   b. Ensure that the passwords are generated by using an Approved block cipher or hash algorithm to combine a symmetric key stored on a personal hardware device with a nonce to generate a one-time password. The nonce may be a date and time, a counter generated on the device, or a challenge from the verifier (if the device has an entry capability); direct electronic input from the device to a computer is also allowed.
   c. Ensure that the one-time password have a limited lifetime, on the order of minutes, although the shorter the better.

4. Password Token

   a. This type of token is a secret that a claimant memorizes and uses to authenticate his or her identity. Passwords are typically character strings, however systems using a number of images that the subscriber memorizes and must identify when presented along with other similar images are also acceptable.

References

FIPS 112, *Password Usage*; FIPS 181, *Automated Password Generator*; FIPS 186-2, *Digital Signature Standard;* NIST SP 800-63, *Electronic Authentication Guideline.*

5.2 Access Control

Procedures

- Establish access control rules to be implemented for each system to ensure only designated individuals, under specified conditions (e.g., time of day, port of entry, type of authentication, etc.) can:

1. Access the information system (e.g., log-on, establish connection).
2. Activate specific system commands.
3. Execute specific programs and procedures.
4. Create, view, or modify specific objects (e.g., programs, information, system parameters).

- Ensure that for information systems employing password-based authentication, passwords are:

1. one-way encrypted for storage
2. transmitted on the network in a secure manner (e.g., encrypted)
3. not displayed when entered
4. controlled by the associated user

- Ensure authentication is required for access to administrative systems from the Internet with the use of passwords as the minimum standard for authentication.
- Establish procedures for obtaining appropriate access controls for all systems within the organization, which require the following:

1. users to provide a list of applications, databases, or external systems required to fulfill their individual or role-based duties
2. verification that the individual needs access to perform duties from the system owner, supervisor, or other appropriate authority
3. a method to ensure separation of duty protocols are enforced in granting access

- Ensure that all Departmental and contractor personnel who are requesting access to MAs and GSSs follow these procedures:

1. Complete a user access registration form.
2. Ensure that system owners review what is being requested and give approval on the form.

- Ensure that access to security software is restricted to security administrators.
- Implement controls to monitor access and identify apparent security violations.
- Ensure appropriate investigation procedures are implemented following security violations.

References

National Security Telecommunications and Information Systems Security Policy (NSTISSP) 200, *National Policy on Controlled Access Protection.*

5.2.1 Review and Validate System User Accounts

Procedures

- Terminate emergency or temporary accounts automatically after one month.
- Disable inactive accounts automatically after one month.
- Ensure the continued need for system access is based on the principles of least privilege and need to know.

    1. An access control list (ACL) must be kept current by adding new users and deleting former users.

- Monitor remote access user profiles for use; if user activity lapses for 60 days, revoke user's privileges.

    1. Remote access use should be monitored periodically, preferably on a daily basis.
    2. Remote access authorizations should be reviewed by the supervisor at least every 60 days to ensure the validity of the user's remote access.
    3. The supervisor should ensure that the CISO receives a copy of this review after each review is completed.

References

NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook*, for further guidance.

5.2.2 Automatic Account Lockout

Procedures

- Lock users out of the system after three consecutive failed log-on attempts.
- To re-access the system, users will need to contact the appropriate system administrator to have access re-instated.

References

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

5.2.3 Automatic Session Lockout

Procedures

- Ensure the information system is configured to activate a password protected “screen saver” option after a maximum of 30 minutes of inactivity and blocks further access until the user re-establishes the connection using the proper identification and authentication procedures.

    1. Based on sensitivity of information on the system, the OPDIV can make the time limit shorter based on their risk based management decision.

- Ensure session-lock functionality is associated with each information system node (e.g., terminal, workstation, notebook computer).

References

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

5.2.4 Warning Banner

Procedures

- Ensure where technically practical, Departmental computers and IT systems display a sign-on warning banner to all users who log on to government computers and systems.
- Ensure orientation and security education or awareness programs for employees include notification of the use of sign-on warning banners on Departmental systems.
- Configure systems to display the required warning banner in accordance with Departmental guidance.

References

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

Refer to appendix K for a sample warning banner.

5.3 Audit Logs

Procedures

- Maintain and protect audit logs for all systems.
- Ensure audit logs record system activity by both system and application

processes and user activities in systems and applications.

- Ensure audit logs record the following events:

  1. start-up and shutdowns of systems or audit functions
  2. successful and unsuccessful login and logout of users
  3. user actions to open, close, create, execute, modify, or delete programs or files
  4. actions taken by system administrators, system security administrators, or other super users
  5. changes or attempts to change privileges and access controls for users and objects.

- Ensure audit logs record the following information for each event:

  1. date and time of the event
  2. type of event
  3. success or failure of the event
  4. name of the program or file introduced, accessed, modified, or deleted.

- Ensure systems are able to associate each auditable event with the individual identity of the user or system process that caused the event.
- Ensure audit logs/records are backed up no less than weekly onto a different information system or media than the system being audited.
- Ensure audit logs are protected as sensitive information and retained for at least six months.
- Ensure system administrators do not have “write” access to audit trails.

  1. A person other than the system administrator must conduct regular analyses of audit trails, although the system administrator may also be permitted to review audit trails.

References

NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook;* NIST SP 800-18, *Guide for Developing Security Plans for Information Technology Systems*.

5.4 Network Security

5.4.1 Remote Access and Dial-In

Procedures

- Limit remote and dial-in access to those personnel with justification for such access.
- Document justification for remote access and secure approval from the designated Departmental official.
- Maintain security standards for remote access.

- Conduct periodic monitoring to ensure installed equipment does not include unanticipated dial-up capabilities.
- Restrict trust relationships among hosts and external entities to the appropriate minimum level necessary to accomplish mission tasks.
- Ensure access to the Internet from home or another location using a Department-owned desktop/laptop computer, through Department-owned connections, or via approved centralized dial-in solutions, adheres to the same policies that apply to use from within Departmental facilities.
- Ensure employees do not allow family members or other non-employees to access Departmental information systems.
- Prohibit the use of desktop modems to support dial-in access to Departmental systems unless using a CISO-approved Virtual Private Network (VPN) solution.

References

NIST SP-800-12, *An Introduction to Computer Security: The NIST Handbook*; NIST SP-800-41, *Guidelines on Firewalls and Firewall Policy*; NIST SP-800-44, *Guidelines on Securing Public Web Servers*; NIST SP-800-45, *Guidelines on Electronic Mail Security.*

5.4.2 Network Security Monitoring

Procedures

- Provide user education and train end users of computing systems to report any anomalies in system performance and security incidents.
- Implement intrusion detection systems (IDS), in addition to firewalls, to monitor the network traffic.
- Maintain a network map, to include:

    1. all active hosts connected to Departmental networks
    2. network services operating on those hosts
    3. the specific application running the identified services

- Perform ongoing security monitoring for vulnerabilities and security problems; some monitoring methods and tools include:

    1. review of system logs
    2. automated tools, such as virus scanners, check summing, integrity verification programs, intrusion detectors, system performance monitoring
    3. configuration management.

References

NIST SP 800-31, *Intrusion Detection Systems*; NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook*; NIST SP 800-28, *Guidelines on Active Content and Mobile Code*; NIST SP 800-44, *Guidelines on Securing Public Web Servers.*

Refer to the *IT Penetration Testing Guide* for further guidance.

5.4.3 Firewall

Procedures

- Configure and patch firewall systems in a timely manner.

    1. Install all available updates and patches for the Departmental firewall operating environment (FOE) operating systems.
    2. Establish a formal change management process for Departmental FOEs or ensure FOEs participate in an existing change management process employed within the Department.
    3. Audit and verify all firewall and security policies at least quarterly.

- Prohibit entry points into the environment that are not controlled and protected by the Departmental FOE.
- Configure Departmental firewall host operating systems with the minimum essential services, privileges, commands, software, and applications that are necessary for firewall operation and maintenance.
- Configure firewalls to allow external access through the fewest ports necessary and establish a "deny all traffic except what is explicitly permitted to accomplish the mission rule set."
- Block any protocol and traffic that is not necessary via use of boundary router and packet filtering technology.
- Develop standard configurations that limit or block network traffic that is considered a security threat to the Department.
- Remove all services that allow remote operation or control of the FOE.
- Protect the firewall system from unauthorized access.
- Use the network time protocol (NTP), or another appropriate mechanism, to synchronize the logs with other logging systems such as intrusion detection.

References

NIST SP 800-7, *Security in Open Systems*; NIST/NSA Publication, *U.S. Government Firewall Protection Profiles for Sensitive Unclassified Environments*; NIST SP 800-28, *Guidelines on Active Content and Mobile Code*; NIST SP 800-41, *Guidelines on Firewalls and Firewall Policy.*

Refer to appendix L for a list of firewall services to block.

5.4.4 Intrusion Detection Systems (IDS)

- Deploy infrastructures to detect intrusions, to analyze and correlate the results, and to react as needed.
- Provide an intrusion detection, reporting, analysis, assessment, and response infrastructure that not only enables rapid detection and response to intrusions

and other anomalous events but also provides operational situation awareness.

References:

NIST SP 800-31, *Intrusion Detection Systems.*

5.4.5 Internet Security

Procedures

- Educate users on the acceptable use of the Internet.

  1. Acceptable use includes activities such as:

     a. Departmental research
     b. mission-related training or current information on issues and events
     c. mission-associated technical or market activities

- Ensure personal accounts are not used for online services from Departmental sites or workstations, and a Departmental subscription or contract agreement must be in place prior to access for any fee-for-use services.
- Disallow unapproved Departmental Web servers.

References

NIST SP 800-7, *Security in Open Systems*; NIST/NSA Publication, *U.S. Government Firewall Protection Profiles for Sensitive Unclassified Environments*.

5.4.6 E-Mail Security

Procedures

- Each OPDIV should automatically deactivate and possibly delete any e-mail accounts not used for a period of 60 days. Deletion should occur after verifying the validity of each account. The OPDIV should develop an account verification process and should put this plan into operation prior to allowing the automatic deactivation process to occur.
- Educate e-mail users on e-mail security, to include:

  1. attachments from unknown senders
  2. attachments with suspicious or known suspect file extensions
  3. e-mails from known senders in which the subject line or content appears to be inappropriate for the existing relationship
  4. scanning all attachments with a virus scanner before opening.

- Update mail clients to the most secure version, including necessary patches.
- Ensure users with access to e-mail signing and encryption technology use that technology to protect e-mail messages when handling sensitive data.

- Restrict the maximum accepted message size on e-mail servers.
- Prevent malicious code from entering the e-mail system by:

  1. filtering potentially dangerous attachment types (e.g., .vbs, .ws, .wsc file extensions) at the mail server or mail gateway
  2. blocking active content (the most popular types of active content are ActiveX, Java, JavaScript, and Visual Basic Script), which often comes in the form of a client side scripting language, or control object.

- E-mail clients, by default, should be configured to the following:

  1. disable automatic message preview
  2. disable automatic opening of next message
  3. disable processing of active content

  Changes to these settings should be prohibited, unless suitable malicious software protections have been implemented.

- Set logging on the mail server to the most detailed level available.

References

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

5.4.7 Personal E-Mail Accounts

Procedures

- Educate users that Departmental communications systems and equipment, including e-mail and Internet systems and their associated hardware and software, are for official and authorized purposes only.
- Ensure Sensitive But Unclassified (SBU) and Privacy Act information is transmitted only in accordance with Departmental policy.

5.4.8 Security Testing and Vulnerability Assessment

Procedures

- Update the list of vulnerabilities scanned periodically, at least prior to each periodic scan.
- Prepare a summary list of vulnerabilities for each information system and facility that is analyzed.
- Use automated vulnerability assessment or state management tools wherever system capabilities permit.
- Conduct routine penetration tests and vulnerability assessments to identify potential weaknesses throughout Departmental MAs and GSSs.

1. Conduct security testing in close coordination with system owners and users.
2. Ensure all systems are fully backed up before vulnerability scanning tools are applied.
3. Determine frequency of scans based on risk.

- Implement security safeguards and mitigation measures to correct or reduce the risks associated with identified security weaknesses.

References

P.L. 107-347 Title III, FISMA; NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook*; NIST SP 800-31, *Intrusion Detection Systems (IDS)*; NIST SP 800-41, *Guidelines on Firewalls and Firewall Policy*; NIST SP-800-42, *Draft Guideline on Network Security Testing*; NIST SP-800-44, *Guidelines on Securing Public Web Servers.*

Refer to the *HHS IT Penetration Testing Guide* for further guidance.

5.5 Cryptography

Procedures

- Ensure encryption is used to protect all sensitive information that is protected under HIPPA and the Privacy Act, as well as all system authentication data (i.e. passwords) and system identification data (i.e., Internet Protocol (IP) addresses, host names).
- Ensure encryption standards use only algorithms that NIST has approved.

References

NIST SP 800-21, *Guideline for Implementing Cryptography in the Federal Government*; FIPS 140-2, *Security Requirements for Cryptographic Modules*; FIPS 197, *Advanced Encryption Standards.*

Refer to *HHS Data Cryptography Guide* for further guidance.

5.6 Malicious Code Protection

Procedures

- Ensure information systems (including servers, workstations and mobile computing devices) implement malicious code protection that includes a capability for automatic updates.
- Ensure virus definitions are up to date.
- Provide virus-scanning software at critical entry points, such as remote-access servers and at each desktop system on the network.

- Ensure antiviral mechanisms are used to detect and eradicate viruses in incoming and outgoing e-mail and attachments.
- Ensure employees and contractors use antivirus software for all IT systems and do not disable such software unless specifically directed by authorized personnel.
- Configure automated virus-scanning software, if used, to scan workstations or hosts at system start up.
- Educate all employees and contractors about the risks of malicious software, available protections against such threats, and the process of reporting suspected incidents.
- Scan all software files intended for Departmental use before use regardless of source.

  1. Policy applies without regard to the physical location of the equipment or software.
  2. Scans must precede vendor demonstrations in all circumstances.
  3. Scans must be done on all vendor-supplied storage media.

- Implement these required actions to reduce the risk of a virus incident:

  1. Make backup copies on diskettes or optical disks of all mission-critical information; two or more copies are preferable, located away from the immediate area of the user’s workstation.
  2. Avoid using demonstration diskettes of commercial or shareware programs.
  3. Use the “write protect” function on any program diskettes and on backup diskettes.

- Scan for viruses immediately after the download process for any type of file downloaded from any network source.

  1. Routine scanning done automatically at log-on is not totally sufficient to prevent virus attacks.
  2. Virus scanning must take place to preclude a virus from working for several hours or overnight before it is discovered.

- Ensure that contract deliveries are virus-free.

  1. IT contracts must include language that requires contractors to deliver all hardware, software, and services free of known viruses.

References

NIST SP 800-5, *Guide to the Selection of Anti-Virus Tools and Techniques*; NIST SP 500-166, *Computer Viruses and Related Threats: A Management Guide*; NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook.*

5.7 Product Assurance

Procedures

- Require the review and approval of the OPDIV CISOs for security considerations of all significant IT procurements.
- Establish and maintain a list of approved or non-approved equipment, based on Department-wide security requirements.
- Ensure that products are selected and implemented in accordance with the requirements outlined in the CCIMB-99-031, Common Criteria for Information Technology Security Evaluation.

References

NIST SP 800-4, *Computer Security Considerations in Federal Procurements: A Guide for Procurement Initiators, Contracting Officers, and Computer Security Officials;* NIST SP 800-23, *Guideline to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products;* NIST SP 800-36, *Guide to Selecting Information Security Products*; CCIMB-99-031, *Common Criteria for Information Technology Security Evaluation.*

Refer to the *IT Security Capital Planning Guide* for further guidance.

5.8 System-to-System Interconnection

5.8.1 Implementation Plan

Procedures

- Develop a system-to-system interconnection implementation plan for each instance of a system-to-system interconnection to centralize all aspects of the interconnection effort in one document and to clarify how technical requirements shall be implemented.
- Ensure the interconnection plan verifies that IT systems are properly and securely connected.
- Develop the interconnection plan through a collaborative effort involving a planning team that is comprised of the appropriate program managers, security officers, system administrators, and network administrators from each system to be connected.
- Ensure the appropriate OPDIV CISOs review and approve the finalized interconnection plan.

References

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

5.8.2 Execute the Implementation Plan

Procedures

- Execute the system-to-system implementation plan for each instance of a system-to-system interconnection after the appropriate OPDIV CISOs have reviewed and approved the plan.
- Ensure the execution of the implementation plan includes:

  1. implementation and configuration of security controls
  2. installation and configuration of hardware and software
  3. integration of applications
  4. operational and security testing
  5. security awareness training.

References

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

5.8.3 Activate the Interconnection

Procedures

- Ensure system owners activate the system-to-system interconnection for use following the established implementation plans.
- Monitor the interconnection for a period of at least three months following activation to ensure that the systems operate properly and securely.
- Ensure that Departmental ISSOs, network administrators, and system administrators analyze audit logs frequently to monitor the types of assistance users request.
- Document and correct all weaknesses or problems that occur in the system interconnection.

References

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

5.9 Peer-to-Peer Software

Procedures

- Configure Departmental networks to disallow peer-to-peer and instant messaging software, or to only allow the secure use of peer-to-peer and instant messaging software.
- Educate users about the Departmental policies related to peer-to-peer and instant messaging software.

References

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

5.10 Patch Management

Procedures

- Educate users about the Department's patch management processes.
- Maintain a list of patches installed.
- Test patches for adverse effects prior to installation across the entire Department.

References

Refer to the *HHS Configuration Management Guide* for additional information on patch management.

Appendix A: Document Feedback Form

This form is for reviewer suggested corrections, revisions, or updates and is intended 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 the Chief Information Officer (OCIO).

By E-mail: SecureOne.HHS@hhs.gov
Subject Line: Guidance Feedback
By Phone: OCIO: (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 are provided because sections in the publication 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.

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

CCIMB-99-031, *Common Criteria for Information Technology Security Evaluation.* August 1999.

Executive Order (E.O.) 12674, *Standards of Ethical Conduct for Employees of the Executive Branch,* April 12, 1989.

E.O. 13231, *Critical Infrastructure Protection in the Information Age*, October 16, 2001.

Presidential Decision Directive (PDD) 63, *Critical Infrastructure Protection*, May 22, 1998.

Homeland Security Presidential Directive (Hspd)-7, *Critical Infrastructure Identification, Prioritization, and Protection,* December 17, 2003.

Federal Information Processing Standard (FIPS) Publication (PUB) 31, *Guidelines for Automatic Data Processing Physical Security and Risk Management,* June 1974.

FIPS PUB 112, *Password Usage,* May 1985.

FIPS PUB 140-2, *Security requirements for Cryptographic Modules,* June 2001.

FIPS PUB 181, *Automated Password Generator,* October 1993.

FIPS PUB 186-2, *Digital Signature Standard,* January 2000.

FIPS PUB 197, *Advanced Encryption Standard,* November 2001.

FIPS PUB 199, *Standards for Security Categorization of Federal Information and Information System*, February 2003.

National Communications System (NCS) Federal Telecommunications Recommendation (FTR), *Video Teleconferencing Services at 56 to 1,920 kbit/s, October 8, 1998.*

National Institute of Standards and Technology (NIST) Special Publication (SP) 500-166, *Computer Viruses and Related Threats: A Management Guide*, August 1989.

NIST SP 800-4A, *Security Considerations in Federal Information Technology Procurements,* March 1992.

NIST SP 800-4, *Computer Security Considerations in Federal Procurements: A Guide for Procurement Initiators, Contracting Officers, and Computer Security Officials,* March 1992.

NIST SP 800-5, *Guide to the Selection of Anti-Virus Tools and Techniques,* December 1992.

NIST SP 800-7, *Security in Open Systems*; NIST/NSA Publication, *U.S. Government Firewall Protection Profiles for Sensitive Unclassified Environments*, July 1994.

NIST SP 800-9, *Good Security Practices for Electronic Commerce,* December 1993.

NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook,* March 1996.

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 800-16, *Information Technology Security Training Requirements, A Role and Performance Based Model,* April 1998.

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

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

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

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

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

NIST SP 800-31, *Intrusion Detection Systems (IDS),* November 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 Technology Security Products*, October 2003.

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

NIST SP 800-41, *Guidelines on Firewalls and Firewall Policy,* January 2001.

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 800-47, *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 800-55, *Security Metrics Guide for IT Systems,* July 2003.

NIST DRAFT SP 800-58, *Security Considerations for Voice Over IP Systems.*

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

NIST SP 800-63, *Electronic Authentication Guideline,* September 2004.

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

National Security Telecommunications and Information Systems Security Policy (NSTISSP) 200, *National Policy on Controlled Access Protection,* July 15, 1987.

National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 1000, *National Information Assurance Certification and Accreditation Process*, April 2000.

General Accounting Office (GAO), *Federal Information System Controls Audit Manual* (FISCAM) (GAO/AIMD-12.19.6, January 1999)

Office of Management and Budget (OMB) Circular A-123; *Management Accountability and Control*, June 21, 1995.

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

OMB Memorandum (M)-97-02, *Funding Information Systems Investments,*
October 25, 1996.

OMB M-97-16, *Information Technology Architectures*, June 18, 1987.

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

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

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

OMB M-03-19, *Memorandum for Heads of Executive Departments and Agencies*, August 2003.

OMB M-03-22, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, September 26, 2003.

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

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

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

Public Law 107-347*, The E-Government Act of 2002, Title III—Information Security,* cited as the *Federal Information Security Management Act of 2002 (FISMA),* December 17, 2002.

Appendix C: Acronyms

ACL	Access Control List
AES	Advanced Encryption Standard
AIS	Automated Information System
BCP	Business Continuity Plan
BI	Background Investigation
BIA	Business Impact Analysis
BIOS	Basic Input/Output Systems
CA	Certification Authority
C&A	Certification and Accreditation
CCB	Configuration Control Board
CCIMB	Common Criteria Interpretations Management Board
CERT	Computer Emergency Response Team
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CISO	Chief Information Security Officer
COMSEC	Communications Security
COOP	Continuity of Operations Plan
CPIC	Capital Planning and Investment Control Process
CRT	Cathode Ray Tube
DAA	Designated Approving Authority
DES	Data Encryption Standard
DOJ	Department of Justice
DoS	Denial of Service
DRAM	Dynamic Random Access Memory
DRP	Disaster Recovery Plan
EAPROM	Electronically Alterable PROM
EEPROM	Electronically Erasable PROM
E.O.	Executive Order
EPROM	Erasable Programmable ROM
FAR	Federal Acquisition Regulation
FedCIRC	Federal Computer Incident Response Center
FEPROM	Flash EPROM
FIPS	Federal Information Processing Standard
FISCAM	Federal Information System Controls Audit Manual
FISMA	Federal Information Security Management Act of 2002
FOE	Firewall Operating Environment
FOIA	Freedom of Information Act
FTR	Federal Telecommunications Recommendation
GAO	General Accounting Office
GSS	General Support System
HHS	Department of Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act of 1996
Hspd	Homeland Security Presidential Directive
IA	Information Assurance

I&A	Identification and Authentication
ID	Identification
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IG	Inspector General
IP	Internet Protocol
IPSO	Information Processing Service Organization
IRT	Incident Response Team
ISDM	Information Security Data Management
ISSO	Information Systems Security Officer
IT	Information Technology
LAN	Local Area Network
MA	Major Application
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
NAC	National Agency Check
NACI	National Agency Check and Inquiries
NCS	National Communications System
NIACAP	National Information Assurance Certification and Accreditation Process
NIPC	National Infrastructure Protection Center
NIST	National Institute of Standards and Technology
NOVRAM	Nonvolatile RAM
NSIRC	National Security Incident Response Center
NSTISSP	National Security Telecommunications and Information Systems Security Policy
NTP	Network Time Protocol
OCIO	Office of the Chief Information Officer
OHR	Office of Human Resources
OIG	Office of the Inspector General
O&M	Operations and Maintenance
OMB	Office of Management and Budget
OPDIV	Operating Division
OPM	Office of Personnel Management
PBX	Private Branch Exchange
PCD	Portable Computing Device
PDD	Presidential Directive Decision
PIA	Privacy Impact Assessment
PL	Public Law
POA&M	Plan of Action and Milestones
PROM	Programmable ROM
PUB	Publication
QoS	Quality of Service
RAD	Rapid Application Development
RAID	Redundant Array of Inexpensive Disks
RF	Radio Frequency
RoB	Rules of Behavior

ROM	Read-Only Memory
RTO	Recovery Time Objective
SBU	Sensitive But Unclassified
SDLC	System Development Life Cycle
SLC	System Life Cycle
SOCC	Secure One Communications Center
SP	Special Publication
SRAM	Static Random Access Memory
SSAA	System Security Authorization Agreement
SSBI	Single Scope Background Investigation
SSN	Social Security Number
SSP	System Security Plan
STAFFDIV	Staff Division
ST&E	Security Test and Evaluation
T&E	Test and Evaluation
VoIP	Voice-Over Internet Protocol
WORM	Write Once, Read Many

Appendix D: Glossary

Acceptable Risk—a concern that is acceptable to responsible management, due to the cost and magnitude of implementing security controls. (Defined in NIST SP 800-26, Appendix C).

Access—ability to make use of any information system (IS) resource. (Defined in NIST 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 nonrepudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action. (Defined in NIST SP 800-30, Appendix E).

Accreditation—the formal declaration by the DAA that a major application or general support system is granted approval to process using a prescribed set of safeguards in a specific operational environment. The accreditation decision is made on the basis of a certification by designated technical personnel that the system meets prespecified technical requirements for achieving adequate security after the implementation of an agreed upon set of security controls. (See also adequate security, authorizing official and certification.) (Defined in NIST SP 800-18, Appendix D).

Assurance—grounds for confidence that the other four security goals (integrity, availability, confidentiality, and accountability) have been adequately met by a specific implementation. “Adequately met” includes (1) functionality that performs correctly, (2) sufficient protection against unintentional errors (by users or software), and (3) sufficient resistance to intentional penetration or bypass. (Defined in NIST SP 800-30, Appendix E).

Asymmetric Cryptography—public-key cryptography; a modern branch of cryptography in which the algorithms employ a pair of keys (a public key and a private key) and use a different component of the pair for different steps of the algorithm. (Defined by SANS at http://www.sans.org/resources/glossary.php#A).

Audit—a formal (usually independent) review and examination of a project or project activity for assessing compliance with contractual obligations. (Defined in Department of Justice (DOJ), System Development Life Cycle (SDLC) Guidance Document, Appendix A).

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 (COMSEC) 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, §3.13.)

Authenticity—the property of being genuine and able to be verified and be trusted; assurance of the validity of a transmission, message, or originator within an information system. (Defined in NIST 800-37, Annex B).

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 NIST 800-37, Annex B).

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

Authorize Processing—a process that occurs when management authorizes, in writing, the operation of a system based on an assessment of management, operational, and technical controls. By authorizing processing in a system, the management official accepts the risks associated with it. (See also acceptable risk and accreditation.) (Defined in NIST SP 800-18, Appendix D).

Authorizing Official—the senior management 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. (Defined in NIST 800-37, Annex B).

Availability—(1) the degree to which a system (or system component) is operational and accessible when required for use [DOJ, SDLC Guidance Document, Appendix A]. (2) Ensuring timely and reliable access to and use of information [44 U.S.C., § 3542].

Awareness—a learning process that sets the stage for training by changing individual and organizational attitudes to realize the importance of security and the adverse consequences of its failure. (Defined in NIST SP 800-16, Appendix C).

Backup—v. to copy software files onto a different media that can be sorted separately from the original files and used to restore the original files, if needed. The act of creating these files. (Defined in DOJ, SDLC Guidance Doc., Appendix A). n. (1) A set of copied files. (2) A dedicated space, i.e., backup facility, held in reserve in case of severe disruption at the original site. See cold site.

Baseline—a work product (such as software or documentation) that has been formally reviewed, approved, and delivered and can only be changed through formal change control procedures. (Defined in DOJ, SDLC Guidance Document, Appendix A).

Biometric—An image or template of a physiological attribute (e.g. a fingerprint) that may be used to identify an individual. Biometrics may be used to unlock authentication tokens and prevent repudiation of registration.

Business Continuity Plan (BCP)—the documentation of a predetermined set of instructions or procedures that describe how an organization's business functions will be sustained during and after a significant disruption. (Defined in NIST 800-34, Appendix E).

Business Impact Analysis (BIA)—an analysis of an information technology (IT) system's requirements, processes, and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption. (Defined in NIST 800-34, Appendix E).

Capital Planning and Investment Control Process (CPIC)—a management process for ongoing identification, selection, control, and evaluation of investments in information resources. The process links budget formulation and execution, and is focused on agency missions and achieving specific program outcomes. (Defined in OMB Circular A-130, (6)(c)).

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. (See also accreditation and authorizing official.) (Defined in NIST SP 800-37, Annex B).

Chain of Custody—the important application of the Federal rules of evidence and its handling. (Defined by SANS at http://www.sans.org/resources/glossary.php#A).

Cold Site—a backup facility that has the necessary electrical and physical components of a computer facility, but does not have the computer equipment in place. The site is ready to receive the necessary replacement computer equipment in the event that the user has to move from their main computing location to an alternate site. (Defined in NIST SP 800-34, Appendix E).

Confidentiality—(1) assurance that information is not disclosed to unauthorized persons, processes, or devices. (2) Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information [44 U.S.C., §3542].

Configuration Management—the discipline of identifying the configuration of hardware and software systems at each life cycle phase for the purpose of controlling changes to the configuration and maintaining the integrity and traceability of the configuration through the entire life cycle. (Defined in DOJ, Systems Development Life Cycle Guidance Document, Appendix A) Configuration items may include hardware, software, firmware, telecommunications, documentation, test, test fixtures, and test documentation.

Contingency Plan—(1) a formal document that establishes continuity of operations processes in case of a disaster. 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).

Continuity of Operations Plan (COOP)—a predetermined set of instructions or procedures that describe how an organization's essential functions will be sustained for up to 30 days as a result of a disaster event before returning to normal operations. (Defined in NIST SP 800-34, Appendix E)

Critical Assets—those physical and information assets required for the performance of the site mission. (Defined in DOJ, SDLC Guidance Document, Appendix A).

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 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).

Denial of Service (DoS)—the prevention of authorized access to resources or the delaying of time-critical operations. (Defined in NIST SP 800-30, Appendix E).

Design Phase—the period in the systems development life cycle during which the designs for architecture, software components, interfaces, and data are created, documented, and verified to satisfy system requirements. (Defined in DOJ, SDLC Guidance Document, Appendix A).

Designated Approving Authority (DAA)—the senior management official who has the authority to authorize processing (accredit) an automated information (major application) or (general support system) and accept the risk associated with the system. (Defined in NIST SP 800-18, Appendix D).

Development Phase—the period in the system development life cycle to convert the deliverables of the Design Phase into a complete system. (Defined in DOJ, SDLC Guidance Document, Appendix A).

Digital Signature—a hash of a message that uniquely identifies the sender of the message and proves the message hasn't changed since transmission. (Defined by SANS at http://www.sans.org/resources/glossary.php#A).

Disaster Recovery Plan (DRP)—a written plan that identifies recovery procedures in the event of natural or man-made disasters or catastrophes affecting the availability of the system. This plan is tested annually to ensure the continued effectiveness and adequacy of the plan. (Defined in NIST SP 800-34, Appendix E).

Disruption—an unplanned event that causes the general system or major application to be inoperable for an unacceptable length of time (e.g., minor or extended power outage, extended unavailable network, or equipment or facility damage or destruction). (Defined in NIST SP 800-34, Appendix E).

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 SANS at http://www.sans.org/resources/glossary.php#A).

Environmental Security—the application of control procedures, conditions, and objects as preventive measures that affect the development, operation, and maintenance of a system. These preventive measures include but are not limited to fire safety and supporting utilities.

Environmental Threat—any surrounding unintentional or natural accident, incident, or malfunction that may cause damage to IT resources, information, and personnel (i.e., structural failure, power fluctuation, temperature/humidity fluctuation, and heating and cooling system failure). (Compare with natural threat.)

Event—an observable occurrence in a network or system

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 OMB Circular A-130, (A)(2)(c))

Hot Site—a fully operational offsite data processing facility equipped with hardware and system software to be used in the event of a disaster. (Defined in NIST SP 800-34, Appendix E). (Compare with warm site and cold site.)

Human Threat—a person or an organization with the capability and intention to do damage to the HHS mission. (Compare to natural threat.)

Implementation Phase—the period in the systems development life cycle when the system is installed, made operational, and turned over to the user (for the beginning of the Operations and Maintenance Phase). (Defined in DOJ, SDLC Guidance Document, Appendix A).

Incident— the violation, or an imminent threat of a violation, of an explicit or implied security policy, acceptable use policies, or standard security practices in a computing or telecommunications system or network. While certain adverse events, (e.g., floods, fires, electrical outages, and excessive heat) can cause system crashes, they are not considered computer-security incidents.

Incident Handling—an action plan for dealing with intrusions, cyber-theft, denial of service, fire, floods, and other security-related events. It is comprised of a six-step process: Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned. (Defined by SANS at Http://www.sans.org/resources/glossary.php#A).

Incident Response Plan—the documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyber attacks against an organization's IT systems(s). (Defined in NIST SP 800-34, Appendix E).

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. (CNSS 4009)

Information Resources—includes both government information and information technology. (Defined in OMB Circular A-130, 6(k)). Information and related resources, such as personnel, equipment, funds, and information technology [44 U.S.C., § 3502].

Information Technology (IT)—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. For purposes of this definition, equipment is used by an OPDIV whether the OPDIV uses the equipment directly or it is used by a contractor under a contract with the OPDIV, which (1) requires the use of such equipment or (2) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. Information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources [40 U.S.C., § 1401]. It does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract. (Defined in the Clinger Cohen Act of 1996, §§5002, 5141 & 5142)

Integrity—(1) the degree to which a system (or system component) prevents unauthorized access to, or modification of, computer programs or data. (Defined in DOJ, SDLC Guidance Document, Appendix A). (2) Guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity [44 U.S.C., § 3542].

IT Contingency Plan—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).

Least Privilege—the principle of allowing users or applications the least amount of permissions necessary to perform their intended function. (Defined by SANS at http://www.sans.org/resources/glossary.php#A).

Life Cycle—all the steps or phases a project passes through during its system life, from concept development to disposition. There are nine life cycle phases in the system development life cycle (SDLC). (Defined in DOJ, SDLC Guidance Document, Appendix A).

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 because of the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to, or modification of, the information in the application. A breach in a major application might compromise many individual application programs and hardware, software, and telecommunications components. Major applications can be either a major software application or a combination of hardware and software in which the only purpose of the system is to support a specific mission-related function. (Defined in NIST SP 800-18). Note: All Federal applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight and should be treated as major. Adequate security for other applications should be provided by security of the systems in which they operate. (Defined in OMB Circular A-130, (A)(2)(d)).

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—techniques and concerns, normally addressed by an organization's management, that focus on the management of security and risk of an IT system. More expressly, actions taken to manage the development, maintenance, and use of the system, including system-specific policies, procedures, and rules of behavior, individual roles and responsibilities, individual accountability and personnel security decisions. (Defined in NIST SP 800-16, Appendix C).

National Agency Check (NAC)—a type of investigation to determine suitability for Confidential and Secret clearances that may involve an FBI check of the candidate's name and fingerprints, and an OPM investigation.

National Agency Check and Inquiries (NACI)—similar to a NAC, but supplemented by a credit check, and written inquiries, which may be sent to schools, former employers, law enforcements agencies or former spouses.

Natural Threat—a threat posed by fire or natural disasters such as tornado, earthquake, or flood. (Compare to environmental threat and human threat.)

Nonrepudiation— Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information. (Defined in NIST 800-37, Annex B).

Operational Controls—procedures and operational methods focusing on mechanisms implemented and executed by people (as opposed to systems). They often require technical or specialized expertise and often rely upon management activities as well as technical controls. (Defined in NIST SP 800-18, Appendix D).

Operations and Maintenance (O&M) Phase—the period of time in the systems development life cycle during which a software product is employed in its operational environment, monitored for satisfactory performance, and modified as necessary to correct problems or to respond to changing requirements. (Defined in DOJ, SDLC Guidance Document, Appendix A).

Password—a string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization. (Defined in FIPS PUB 140-2).

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 NCSC-TG-004).

Phase—a defined stage in the systems development life cycle; there are nine phases in the full, sequential life cycle. (Defined in DOJ, SDLC Guidance Document, Appendix A).

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)—(also referred to as a corrective action plan) a tool that identifies tasks that need to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the task, and scheduled completion dates for the milestones. The purpose of the POA&M is to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems. (Defined in OMB Memorandum 02-01).

Policy—the rules and regulations set by the organization. Policy determines the type of internal and external information resources employees can access, the kinds of programs they may install on their own computers as well as their authority for reserving network resources. Policy is also related to network quality of service (QoS), because it can define priorities by user, workgroup or application with regard to reserving network bandwidth. (Defined by TechWeb at http://www.techweb.com/encyclopedia).

Privacy—restricting access to subscriber or Relying Party information in accordance with Federal law and Agency policy. (Defined in NIST SP 800-32, Section 9).

Private Key—a cryptographic key used with a public key cryptographic algorithm, uniquely associated with an entity, and not made public. (Defined in FIPS PUB 140-2).

Public Key—the portion of a key pair that is available publicly. (Defined by Entrust at http://www.entrust.com/resources/glossary.htm). The publicly disclosed component of a pair of cryptographic keys used for asymmetric cryptography. (See also key pair.) (Defined by SANS at http://www.sans.org/resources/glossary.php#A).

Project Manger—the person with the overall responsibility and authority for the day-to-day activities associated with a project. (Defined in DOJ, SDLC Guidance Document, Appendix A).

Public Key Encryption—the popular synonym for “asymmetric cryptography.” (See also key pair.) (Defined by SANS at http://www.sans.org/resources/glossary.php#A).

Rapid Application Development (RAD)—in a RAD work pattern, the Requirements Definition and Design phases are iteratively conducted; in this process, a rough set of requirements is used to create an initial version of the system, giving users visibility into the look, feel, and system capabilities. User evaluation and feedback provide revisions to the requirements, and the process is repeated until the requirements are considered complete. (Defined in DOJ, SDLC Guidance Document, Appendix A).

Recovery Time Objective (RTO)—the longest time in which a function can be disrupted before serious impacts are experienced.

Residual Risk—the risk remaining after the implementation of new or enhanced security controls in the information system. (Defined in NIST SP 800-30, Section 4.6).

Risk—the net mission impact considering (1) the probability that a particular threat-source will exercise (accidentally trigger or intentionally exploit) a particular information system vulnerability and (2) the resulting impact if this should occur. (Defined in NIST SP 800-30, Appendix E).

Risk Assessment—the process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and additional safeguards that would mitigate this impact. Part of Risk Management and synonymous with Risk Analysis. (Defined in NIST SP 800-30, Appendix E).

Risk Management—the total process of identifying, controlling, and mitigating information system-related risks. It includes risk assessment; cost-benefit analysis; and the selection, implementation, testing, and security evaluation of safeguards. This overall system security review considers both effectiveness and efficiency, including impact on the mission and constraints due to policy, regulations, and laws. (Defined in NIST SP 800-30, Appendix E).

Rules of Behavior (RoB)—rules of behavior are 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).

Security Costs—(also referenced as “resources Required”) in determining information and IT security costs, Federal agencies must consider the following criteria to determine security costs for a specific IT investment:

1. The products, procedures, and personnel (Federal employees and contractors) that are primarily dedicated to or used for provision of IT security for the specific IT investment. Do not include activities performed or funded by the agency Inspector General. This includes the costs of:

- risk assessment
- security planning and policy
- certification and accreditation
- specific management, operational, and technical security controls (to include access control systems as well as telecommunications and network security)
- authentication or cryptographic applications
- education, awareness, and training
- system reviews/evaluations (including security control testing and evaluation)
- oversight or compliance inspections
- Development and maintenance of agency reports to OMB and corrective action
- plans as they pertain to the specific investment
- contingency planning and testing
- physical and environmental controls for hardware and software
- auditing and monitoring

- computer security investigations and forensics
- reviews, inspections, audits and other evaluations performed on contractor facilities and operations.

2. Other than those costs included above, security costs must also include the products, procedures, and personnel (Federal employees and contractors) that have as an incidental or integral component, a quantifiable benefit to IT security for the specific IT investment. This includes system configuration/change management control, personnel security, physical security, operations security, privacy training, program/system evaluations whose primary purpose is other than security; systems administrator functions; and, for example, system upgrades within which new features obviate the need for other stand-alone security controls. (Defined in FY04 OMB Circular A-11, § 53).

3. Many agencies operate networks, which provide some, or all, necessary security controls for the associated applications. In such cases, the agency must nevertheless account for security costs for each of the application investments. To avoid "double-counting," agencies should appropriately allocate the costs of the network for each of the applications for which security is provided. In identifying security costs, some agencies find it helpful to ask the following simple question: If there was no threat, vulnerability, risk, or need to provide for continuity of operations, what activities would not be necessary and what costs would be avoided?

Investments that fail to report security costs will not be funded; therefore, if the agency encounters difficulties with the above criteria, they must contact OMB prior to submission of the budget materials.

Security Test & Evaluation (ST&E)—an examination and analysis of the security safeguards of a system as they have been applied in an operational environment to determine the security posture of the system. (Defined in NCSC-TG-004).

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).

Single Scope Background Investigation (SSBI)—a type of investigation to determine suitability for Top Secret clearances. An SSBI includes elements of the NAC and NACI, but conducts interviews (with the candidate and others) in place of written inquiries and may require a polygraph examination or other psychological evaluations.

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. (Defined in DOJ, Systems Development Life Cycle Guidance Document, Appendix A); (2) The interconnected set of information resources under the same direct management control, which share common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.

System Administrator—the person responsible for planning a system installation and use of the system by other users. (Defined in DOJ, SDLC Guidance Document, Appendix A).

System Concept Development Phase—the phase that begins after the need or opportunity has been identified in the Initiation Phase. The approaches for meeting this need are reviewed for feasibility and appropriateness (for example, cost-benefit analysis) and documented in the System Characterization Document. (Defined in DOJ, SDLC Guidance Document, Appendix A).

System Development Life Cycle (SDLC)—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 and in DOJ, SDLC Guidance Document, Appendix A).

Systems of Records Notice—a notice that is required to be published for any system that has been determined to be an official System of Records (in terms of the criteria established by the Privacy Act). (Defined in DOJ, SDLC Guidance Document, Appendix A).

System Security Plan (SSP)—a document that provides a system security description, and defines the Operational, Management and Technical controls for the system. Security plans define how a system will implement the security policy. The security plan outlines responsibilities for all system users and describes the rules of behavior for those users. For General Support Systems: System security plans must include: 1) a set of rules of behavior concerning use of, security in, and the acceptable level of risk for, the system; 2) required training for all users to ensure security responsibilities are met; 3) personnel controls; 4) an incident response capability to share information concerning common vulnerabilities and threats; 5) continuity of support; 6) cost-effective technical security products and techniques; and 7) written management authorization, based upon the acceptance of risk to the system, prior to connecting with other systems. (Source: OMB Circular A-130, Appendix III, (A)(3)(a)(2)(a-g)).

For Major Applications: Application security plans must include: 1) a set of rules concerning use of and behavior within the application; 2) specialized training for all individuals prior to access that is focused on their responsibilities and the application rules; 3) personnel security controls; 4) contingency planning; 5) appropriate security controls; 6) appropriate rules garnering the sharing of information from the application; and 7) public access controls where an OPDIV application promotes or permits public access. (Source OMB Circular A-130, Appendix III, (A)(3)(b)(2)(a-g)).

Security Program Agencies shall implement and maintain a program to assure that adequate security is provided for all agency information collected, processed, transmitted, stored, or disseminated in general support systems and major applications. Each agency's program shall implement policies, standards and procedures that are consistent with government-wide policies, standards, and procedures issued by the Office of Management and Budget, the Department of Commerce, the General Services Administration, and the Office of Personnel Management. Different or more stringent requirements for securing national security information should be incorporated into agency programs as required by appropriate national security directives. At a minimum, agency programs shall include the following controls in their general support systems and major applications: 1) assign responsibility for security; 2) have a security plan for all systems and major applications; 3) provide for the review of security controls; and 4) require authorization before processing. (Defined in OMB Circular A-130, Appendix III, (A)(3)).

Technical Controls—automated, technological security mechanisms the IT system executes. The controls can provide automated protection for unauthorized access or misuse and facilitate detection of security violations. (See also communications security, and computer security.) (Defined in NIST SP 800-18, Appendix D).

Threat—any circumstance, event, or act that could cause harm to the Department by destroying, disclosing, modifying, or denying service to automated information resources. (See also environmental threat, human threat and natural threat.) (Defined in NIST SP 800-30, Appendix E).

Token-Something that the claimant possesses and controls (typically a key or password) used to authenticate the claimant's identity.

Trojan Horse—a computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program. (Defined by SANS at http://www.sans.org/resources/glossary.php#A)

User—person or process accessing an automated information system (AIS) 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). (Defined in DOJ, SDLC Guidance Document, Appendix A).

Validation—the process of determining the correctness of the final product, system, or system component with respect to the user's requirements. Answers the question, “Am I building the right product?” Compare to verification. (Defined in DOJ, SDLC Guidance Document, Appendix A).

Verification—the process of determining whether the products of a life cycle phase fulfill the requirements established during the previous phase; answers the question, "Am I building the product right?" Compare to validation. (Defined in DOJ, SDLC Guidance Document, Appendix A).

Vulnerability—a flaw or weakness in a system's security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy. (Defined in NIST SP 800-47, Appendix D).

Appendix E: Information Security Program Documents

The Department of Health and Human Services (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
- Baseline Security Requirements Guide
- Certification and Accreditation Guide
- Configuration Management Guide
- Contingency Planning for Information Security Guide
- Critical Infrastructure Protection Planning Guide
- Data Cryptography Guide
- Health Insurance Portability and Accountability Act Compliance Guide
- Incident Response Guide
- Information Technology Penetration Guide
- IT Personnel Security Guide
- IT Physical and Environmental Security Guide
- IT Security Capital Planning Guide
- IT Privacy Impact Assessment Guide
- Plan of Action and Milestones Guide
- Risk Assessment Guide
- System Inventory Guide
- Web Security Guide
- Wireless Security Guide

Appendix F: Non-Disclosure Agreement Form

**NON-DISCLOSURE AGREEMENT FOR HEALTH AND HUMAN SERVICES
CHIEF SECURITY OFFICER
SUPPORT CONTRACT No. GS-35F-0306J**

I will not disclose proprietary information and information designated "For Official Government Use Only," which has been received in connection with the Health and Human Service's Chief Information Security Officer (CISO) Support Contract, except on a need-to-know basis as instructed by the client. I understand that my obligation not to disclose information applies to information, which I have already received and to information I will receive in the future.

More specifically, I will not disclose any sensitive, proprietary information or information designated for official Government use only. Prior to any disclosure to any other Government personnel or any other support contractor personnel, I will verify with the Contracting Officer or CISO that the individual has signed a non-disclosure agreement with the Contracting Officer or CISO substantially the same as this agreement. I understand that unauthorized disclosure of any information designated for official Government use only or HHS-sensitive information, proprietary information or information designated for official Government use only may subject me to disciplinary or adverse administrative action.

______________________________ Name	______________________________ Signature
______________________________ Position/Title	______________________________ Date
______________________________ Organization	

Appendix G: Rules of Behavior

Rules of Behavior (RoB) provide general instructions on the appropriate use of Departmental IT resources and apply to all Departmental users, including both civil servants and contractors. All government and contractor staff are required to read this document and sign and submit the accompanying form before accessing Departmental systems and or networks.

The *HHS Rules of Behavior* are not to be used in place of existing policy. Rather, they are intended to supplement the *HHS Information Security Program Policy* and the *HHS Information Security Program Handbook*. Because written guidance cannot cover every contingency, Departmental staff and users are asked to augment these rules and use their best judgment and highest ethical standards to guide their actions. Because these principles are based on federal laws and regulations, and Departmental regulations and directives, there are consequences for failure to comply with the principles of behavior. Violation of these rules may result in suspension of access privileges, written reprimand, suspension from work, demotion, and criminal and civil penalties.

All government and contractor staff must sign this form, acknowledging that they have been made aware of and understand the requirements and responsibilities outlined in this document. Questions about these ROB may be directed to one's supervisor or Contracting Officer's Technical Representative (COTR), or to the Operating Division (OPDIV) Chief Information Security Officer (CISO).

Activities on Departmental network system resources are subject to monitoring, recording, and periodic audits. Authorized IT security personnel may access any "user's" computer system or data communications and disclose information obtained through such auditing to appropriate third parties (e.g., law enforcement personnel). Use of Departmental IT system resources expresses consent by the user to such monitoring, recording, and auditing.

The signed acknowledgement should be submitted to the supervisor or COTR.
Each supervisor will be required to file all forms with the OPDIV CISO on an annual basis. On an annual basis, the OPDIV CISOs will be responsible for reporting to the HHS CISO the number of personnel who have been authorized to access Departmental systems and the number and percent of whom have signed the acknowledgement form.

The following pages outline the RoB for several key areas of the Departmental Information Security Program. Please note that these lists are not exhaustive.

E-mail

Government-provided e-mail is intended for official use and authorized purposes. E-mail users must exercise common sense, good judgment, and propriety in the use of government-provided resources. Departmental staff and users who misuse government resources in any way may have e-mail privileges withdrawn and may be subject to disciplinary action. Guidance for e-mail use is listed below.

- Limited personal use of Departmental e-mail services is acceptable as long as it does not affect the mission of the Department and does not conflict with laws, regulations, and policies.
- Personnel using Departmental e-mail must give consent to having their e-mail monitored. E-mail contents will not be accessed or disclosed other than for security purposes or as required by law.
- Users shall ensure that e-mail communications are free of viruses through regular screening of incoming e-mail traffic and virus-detection updates.
- E-mail spamming (unsolicited commercial e-mail)—sending or forwarding chain letters, other junk e-mail, or inappropriate messages— is not permitted.
- The sending of threatening, obscene, harassing, intimidating, abusive, or offensive material about others is not permitted.
- The use of abusive or objectionable language in either public or private messages is not permitted.
- The sending of messages in support of a “for profit” activity is not permitted.
- The sending of e-mail messages for the purposes of prohibited partisan political activity is not permitted. Prohibited partisan political activity is any activity restricted under the Hatch Act.
- The transmission of confidential or sensitive information by e-mail, unless protected by Departmental-approved encryption, is not permitted.
- E-mail software should not be left open on computer systems to prevent unauthorized access and misuse.
- Unauthorized Government-wide or agency-wide broadcast messages are not permitted.
- Distribution of unauthorized newsletters is not permitted.

Internet

Government-provided Internet access is intended for official use and authorized purposes. Internet users must exercise common sense, good judgment, and propriety in the use of government-provided resources. Departmental staff and users who misuse government resources in any way may have Internet privileges withdrawn and may be subject to disciplinary action. Guidance for Internet use is listed below.

- Limited personal use is acceptable as long as it does not affect the mission of the HHS and does not conflict with laws, regulations, and policies.
- Personnel using Departmental Internet access must give consent to have their actions monitored. Monitoring will not be performed, or its findings disclosed, for reasons other than for security purposes or required by law.
- The act of, or the attempt to, break into another computer (federal or private) or introducing malicious code (e.g., computer viruses, worms, or Trojan horses) is not permitted.
- Certain types of data, such as personal or unauthorized government owned, or non-government owned software is not permitted.
- It is not permitted to send, retrieve, view, display, or print sexually explicit, suggestive text or images, or other offensive material.
- The use of another person’s account or identity is not permitted.
- The use of Internet games and chat rooms are not permitted.

Passwords

Passwords are an important aspect of computer security and are the front line of protection for user accounts. Listed below are the password requirements to be used for Departmental information systems.

- Create passwords with a minimum of eight characters.

Use a combination of alpha, numeric, and special characters for passwords, with at least at least one uppercase letter, one lower case letter, and one number.

- Avoid using common words found in a dictionary as a password.
- Avoid obvious readable passwords or passwords that incorporate personal data elements (e.g., user's name, date of birth, address, telephone number, or social security number; names of children or spouses; favorite band, sports team, or automobile; or other personal attributes).
- Change passwords every 90 days.
-
    - The password expiration is a risk based management decision and OPDIVs are encouraged to require a shorter time period for password expiration for more sensitive information.

- Change vendor-supplied passwords immediately.
- Do not reuse passwords.

    - A new password must contain no more than five characters from the previous password.

- Protect passwords by committing them to memory or storing them in a safe place:

    - Do not post passwords.
    - Do not keep a password list in an obvious place, such as under keyboards, in desk drawers, or in any other location where it might be disclosed.

- Change password immediately if password has been seen, guessed or otherwise compromised.
- Keep user identifications (ID) and passwords confidential.
- Do not accept another user's password, even if offered.
- Report any compromise or suspected compromise of a password.

    - Report incidents to the Secure One Communications Center (SOCC).
    - All parties shall work to preserve evidence of computer crimes in accordance with Departmental guidance.

Equipment

Government-provided equipment is intended for official use and authorized purposes. For the Departmental RoB, there is no distinction between stand-alone and on-line computer systems. Users must exercise common sense, good judgment, and propriety in the use of government-provided resources. Departmental staff and users who misuse government resources in any way may have equipment privileges withdrawn and may be subject to disciplinary action. Guidance for equipment use is listed below.

- Using Department-provided equipment is restricted to business purposes.
  - Limited personal use is acceptable as long as it does not affect the mission of the Department and does not conflict with laws, regulations, and policies; however, keeping family or personal records, playing computer games, or loading unauthorized software onto government computers is not permitted.
- Personnel using Departmental equipment must give consent to have their actions monitored. Monitoring will not be performed, or its findings disclosed, for reasons other than security purposes or required by law.
- Equipment, software, or computers using locks or an operating system password should not be reconfigured unless operating under Department-approved and applicable standard procedures.
- Protect passwords, information, equipment, systems, and networks to which a user has access.
- Minimize the threat of viruses by write-protecting diskettes, checking "foreign" data for viruses, and never circumventing the anti-virus safeguards of the system.
- Do not leave terminals unattended without password protecting them.
- Report lost or stolen equipment, security incidents, or anything unusual or suspicious immediately to the appropriate OPDIV CISO.

Removal of Equipment

Property passes are to be obtained from the Property Custodial Officer before the removal of any Departmental network equipment from the building.

Software Licensing

Copyright laws and the license agreements accompanying the software on Departmental equipment govern Departmental users' acquisition and use of software. It is the responsibility of all Departmental staff and users to protect Departmental interests in the performance of their duties. This includes responsibility for assuring that commercial software, acquired by Departmental, is used only in accordance with licensing agreements. Likewise, it is also the Department staff and users' responsibility to assure that any proprietary software is properly licensed before being installed on Departmental equipment. Local Area Network (LAN) and personal computer (PC) users are not to download LAN-resident software. All Departmental staff and users should be aware that it is illegal to:

- copy or distribute software or its accompanying documentation, programs, applications, data, codes, and manuals without permission or a license from the copyright owner
- encourage, allow, compel, or pressure, either explicitly or implicitly, operations staff and users to make or distribute unauthorized software copies
- infringe upon the laws against unauthorized software copying because someone requests or compels it
- loan software so that a copy can be made
- make, import, possess, or deal with articles intended to facilitate the removal of any technical means applied to protect the software program.

Furthermore, according to the United States copyright law, persons violating software licensing laws can be subject to civil damages and criminal penalties.

Departmental software rules are as follows:

- Software will not be modified without the approval of both the development team and the Department.
- Software will only be issued, and used by, authorized individuals as prescribed by local authority.
- The addition of personal IT resources to existing Departmental IT resources without written authorization from the OPDIV CISO is not permitted.
- Security features and controls will be activated when processing data.
- Departmental staff and users aware of any misuse of Departmental software shall notify their supervisor, the security manager, or the OPDIV CISO.

Off-Site Computing

Access to Departmental infrastructure via dial-up or broadband connection poses additional security risks, but may be necessary for certain job functions. Since off-site access is allowed, telecommunication logs and Departmental phone records will be reviewed regularly and routine spot checks will be conducted to determine if Departmental business functions are complying with controls placed on the use of off-site access connections. Access to Departmental networks from off-site locations will be monitored by an audit trail security system.

Government-provided off-site access is intended for official use and authorized purposes. Off-site users must exercise common sense and good judgment in the use of government-provided resources. Departmental staff and users who misuse government resources in any way may have off-site access privileges withdrawn and may be subject to disciplinary action. Guidance for off-site access is listed below.

- The Department provides off-site access to personnel for business purposes.
-
    - Limited personal use is acceptable as long as it does not affect the mission of the HHS and does not conflict with laws, regulations, and policies; however, persons other than the authorized HHS user should not be permitted to make use of HHS equipment and/or software.

- Personnel using Departmental off-site access must give consent to having their actions monitored. Monitoring will not be performed or its findings disclosed other than for security purposes or as required by law.
- Departmental staff and users must adhere to the letter and spirit of all applicable federal laws, regulations, contracts, licenses, policies, standards, guidelines, business controls, security rules, and other expectations.
- Departmental staff and users must report lost or stolen equipment, security incidents or anything unusual or suspicious immediately to their appropriate CISO.
- Departmental staff and users must ensure integrity of data created, accessed, or modified.
- Departmental staff and users must provide a secure and protected environment for government data and government-owned computing resources.
- Departmental staff and users must apply required safeguards to protect government/Departmental records from unauthorized disclosure or damage.

Media Control

Departmental staff and users must adhere to Department-wide procedures for access, storage, and transportation of all media containing sensitive information. Procedures include completing logs to track deposits and withdrawals of media from on-site storage facilities, libraries and backup storage facilities, and procedures for the proper wrapping and labeling of media to be mailed or couriered, or the eventual disposal of media.

HHS staff and users who misuse government resources in any way may have media access privileges withdrawn and may be subject to disciplinary action. Guidance for media control is listed below.

- Departmental staff and users should not leave sensitive information, even temporarily, and should monitor it in the following ways:

  - Departmental staff and users must keep sensitive material in a secure safe or locked cabinet and return all sensitive information to the safe at the end of each business day.
  - Departmental staff and users must abide by the physical and environmental protection controls relating to sensitive data that is contained in a media storage vault or library.
  - Departmental staff and users must turn over, place out of sight, or remove from the screen sensitive information when visitors are present.
  - Departmental staff and users must sanitize or destroy diskettes and other magnetic storage media that contain sensitive data when they are no longer needed to store the sensitive data.
  - Departmental staff and users must dispose of both electronic and hard copy media in accordance with Departmental sanitation and disposal policy.

Voice and Data (Fax) Communication

Government-provided voice communication resources are intended for official use and authorized purposes. Departmental staff and users must exercise common sense and good judgment in the use of all voice communication tools. Departmental staff and users who misuse government resources in any way may have privileges withdrawn and may be subject to disciplinary action. Guidance for voice communication is listed below.

- The Department provides voice communication access to personnel for business purposes.
-
  - Limited personal use is acceptable as long as it does not affect the mission of the Department and does not conflict with laws, regulations, and policies.

- Personnel using Departmental voice communication and facsimile resources consent to having their actions monitored. Monitoring will not be performed, or its findings disclosed other than for security purposes or as required by law.
- Attempting to break into another's voice mail (federal or private) is not permitted.
- Sending threatening, obscene, harassing, intimidating, abusive, or offensive material to or about others is not permitted.
- Using abusive or objectionable language in either public or private messages is not permitted.
- Sending messages in support of a "for profit" activity is not permitted.
- Sending or relaying sensitive information over an unencrypted line is not permitted.
- Sending messages for the purposes of prohibited partisan political activity is not permitted. Prohibited partisan political activity is any activity restricted under the Hatch Act.
- Unauthorized government-wide or agency-wide broadcast messages are not permitted; and distribution of unauthorized messages is not permitted.

Physical Security

Physical access points to sensitive facilities, or restricted areas housing information systems that process or display information are controlled during working hours and guarded or locked during nonworking hours. Access authorization will always be verified before granting physical access and unauthorized personnel are denied access to areas containing protected information. Appropriately authorized personnel are granted physical access, with escort if necessary, to facilities. Departmental staff and users should wear identification badges at all times.

Departmental staff and users who misuse government resources in any way may have their physical access privileges withdrawn and may be subject to disciplinary action. Guidance for physical security is listed below.

- Only authorized Departmental personnel are allowed to re-enter sensitive facilities and restricted/controlled areas containing information systems and system/media libraries after an emergency-related event (e.g., fire drills, evacuations).
- Departmental users not on the access roster for a limited access room or facility must sign in and be escorted the entire time present in the room or facility.
- All Departmental visitors, contractors, or maintenance personnel must be authenticated through preplanned appointments and ID checks.
- Departmental staff and users should inform physical security officials when a system's sensitivity level requires additional protections and alert physical security leadership to locations that house sensitive equipment.
- Departmental staff and users must report immediately any theft or loss of sensitive equipment to physical security personnel.

Disciplinary Action

The Department has established procedures for disciplinary actions for security violations its staff and users commit. These disciplinary actions may be based on the sensitivity of information involved and the number of prior offenses.

The Department has defined remedial actions for employees to include reassignment of work duties, disqualification from a particular assignment, letter of warning, suspension, and/or termination.

It is expected that Departmental staff and users exercise common sense, good judgment, and propriety in the use of Government-provided resources. Departmental staff and users who misuse government resources in any way may be subject to disciplinary action. Guidance for violation handling is listed below.

- Departmental staff and users must report suspected personnel security violations to the Office of Inspector General (OIG) for investigation and recommended disciplinary action.
- Departmental staff and users are subject to disciplinary actions for security violations specified in security awareness training and the Rules of Behavior.
- The Department may remove contractor staff that commit security violations commensurate with high risk to the Department from the contract, and depending on the security violation, criminal sanctions may also apply.
- Departmental staff and users who purposely disclose their passwords to others to share or transfer access are subject to disciplinary actions.
- Departmental users and staff should be alert to developments, such as a drastic change(s) in work habits, which may increase the potential for security violations, whether intentional or accidental.
- Departmental employees and contractors should be aware that any use of the Internet or e-mail that is illegal, offensive, or in violation of Departmental policies or standards can be the basis for disciplinary action up to and including legal action.
- Departmental staff and users should not allow, encourage, or promote the illegal duplication of software in their possession.
- Departmental staff and users, who purposely make, acquire, or use unauthorized copies of computer software, may be subject to disciplinary action.

Incident Reporting Escalation

The Department has established procedures for incident and violation handling that its staff and users might identify to limit any compromises to the Department. Guidance for incident and violation handling is listed below:

- Departmental users must report any of the following incidents to the Secure One Communications Center (SOCC):

  - malicious code: a virus, worm, Trojan horse, or other code-based entity that is either successful or unsuccessful in infecting a host. This category applies to incidents and events.
  - probes and reconnaissance scans: involve searching the network for critical services or security weaknesses.
  - inappropriate usage: a person violates acceptable computing use policies, such as sending spam, email threats, or making illegal copies of software.
  - unauthorized access: a person gains logical or physical unauthorized access to a network, system, application, data, or other resource. This access may include root compromises, unauthorized data alterations, Web site defacements, loss/theft of equipment, unauthorized use of passwords, and use of packet sniffers.
  - denial of service (DoS) attacks: a successful or unsuccessful attack (including Distributed Denial of Service Attacks) impairs the authorized use of networks, systems, or applications by exhausting resources, to include Distributed DoS attacks.
  - other types of incidents include, but are not limited to:

    - alterations/compromises of information
    - adverse site mission impacts
    - classified system incidents
    - loss or theft of equipment.

- Reporting incidents to the SOCC can be made by phone, email, or through ISDM.

  - E-mail address is: Security.CommunicationsCenter@hhs.gov
  - Phone number is: 202-205-9581
  - ISDM address is: https://intranet.hisp.hhs.gov/hhs/public.

- Departmental users should report these incidents within a 2-hour time frame of the incident occurring.
- All Departmental users and staff should be trained on the appropriate incident-response handling procedures.

Education and Awareness

The Department has established procedures for ensuring its staff and users receive education and awareness training. Guidance on education and awareness is listed below:

- All Departmental users, including contractors, must receive education and awareness training commensurate with their duties.
- All new Departmental users of IT systems must receive initial training before being authorized network access and within 60 days of appointment.
- All Departmental users must receive annual refresher training.

SIGNATURE PAGE

All government staff and contractors are required to read the Rules of Behavior and are responsible for abiding by its contents. Violations of the Rules of Behavior or computer policies may lead to disciplinary action, up to and including termination of employment. Signing this form acknowledges your understanding of the requirements for access to Departmental IT systems and your responsibilities as a system user.

Signatures:

Employee's/User's Name: ______________________________
(Print)

Organization: ______________________________

Employee's/User's Signature: ______________________________

Date Signed: ______________________________

Supervisor's Name: ______________________________
(Print)

Supervisor's Signature: ______________________________

NOTE: Sign and return this form to your supervisor or COTR. Make a copy for your records and post it in an accessible area. Your supervisor will retain your original, signed acknowledgement form.

Appendix H: Security Staff Separation Checklist

Access Termination Checklist for Departing Operational Staff

____
(System name)

Departing Staff Member's Name:________________________Separation Date:__________

Action	Completed
Physical Access	
Collect all keys, key cards, and authentication devices that provide access to OPDIV IT facilities.	□
Collect identification card *(unless staff member is remaining within Department).*	□
Change all manual locks for which keys cannot be recovered.	□
Recode all electronic and cipher locks.	□
Collect all equipment, including laptop computers, personal digital assistants, cell phones, and pagers.	□
Report the departure to all staff and regional points of contact.	□
Update all access authorization lists.	□
Computer Access	
Catalog all systems that the staff member was authorized to access and delete their accounts. This should include accounts for the following:	
Remote dial-up access	□
Virtual Private Networking	□
Administrative systems or databases	□
Switches, routers, firewalls, hubs	□
Servers	□
Other (specify):	□
Other (specify):	□
Delete all accounts that are shared by multiple users. Create individual accounts for remaining staff.	□
Match the ownership of each remaining Administrative or Root account to an authorized user. Delete any duplicate or unidentified accounts.	□
Ensure that relevant "guest" accounts are deleted.	□
Involuntarily Terminated Staff (at discretion of CISO)	
Change dial-up numbers for critical infrastructure components.	□
Change authorizing modem strings for connecting to critical infrastructure components.	□
Store all existing access logs for the staff member's accounts.	□
Analyze the final month's access logs for the staff member's accounts.	□
Update antivirus software.	□

Signature:_____________________________________ Date:_____________________
(Supervisor of the departing staff member)

—Retain this completed checklist—

Appendix I: Cleaning and Sanitization Matrix

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

Table Key

(a) Degauss with a Type I degausser. Type I degaussers are equipment rated to degauss magnetic media having a maximum coercivity of 350 Oersteds.

(b) Degauss with a Type II degausser. Type II degaussers are equipment rated to degauss magnetic media having a maximum coercivity of 750 Oersteds.

(c) Overwrite all addressable locations with a single character.

(d) Overwrite all addressable locations with a character, its complement, and then a random character. Verify. This method is NOT approved for sanitizing media containing Top Secret information.

(e) Overwrite all addressable locations with a character, its complement, and then a random character.

(f) Each overwrite must reside in memory for a period longer than the period during which the classified data resided.

(g) Remove all power including battery power.

(h) Overwrite all locations with a random pattern, all locations with binary zeros, and all locations with binary ones.

(i) Perform a full chip erase as directed by the manufacturer's data sheets.

(j) Perform (i) above, then (c) above, for a total of three times.

(k) Perform an ultraviolet erase as directed by the manufacturer's data sheets.

(l) Perform (k) above, but increase the time by a factor of three.

(m) Destroy—disintegrate, incinerate, pulverize, shred, or melt.

(n) Perform the required destruction only if classified information is contained.

(o) Run five pages of unclassified text (font test acceptable).

(p) Destroy ribbons and clean platens.

(q) Inspect and/or test screen surface for evidence of burned-in information. If a CRT is present, it must be destroyed.

Appendix J: Media Disposal Checklist

Media Disposal Checklist for HHS Equipment

Media Description (Include make and model if applicable.):________________________

System Name: ____

Serial Number: ____

Removal From Service Date:____

□ For Destruction □ For Surplus □ For Reuse Disposition* (See checklist.):

Action	Completed
Remove media from operating environment and mark "Removed from Service."	□
Store removed media in a secure location before sanitizing.	□
Determine the disposition of the media by considering the following:	
□ Sensitivity of data	□
□ Ability to render the data unreadable	□
□ Continued need for the media item	□
Mark media with appropriate disposition	□
□ Use overwriting software on the media. *Name and version of software used:*	□
□ Use a degausser on media containing highly sensitive data. *Brand and coercivity of degausser used:*	□
Verify that media is unreadable:**	□
□ If not unreadable, repeat degaussing.	□
□ If degaussing fails, mark media "For Destruction."	□
If media is to be destroyed:	
□ Mark "For Destruction."	□
□ Notify inventory representative for removal of media.	□
If media is to be surplused:	
□ Mark "For Surplus—Sanitized."	□
□ Notify inventory representative for removal of media.	□
If media is to be reused:	
□ Mark "For Reuse—Sanitized."	□
□ Return media to production environment or place in storage.	□
Update configuration management plan.	□
Retain the completed checklist in the sanitization log.	□

Signature:______________________________ Date:________
Verifier Signature:______________________ Date:________

** *A trained individual other than the one who performed the sanitization process should perform verification on a random basis.*

Appendix K: Warning Banners

Example of Internal Warning Banner

WARNINGWARNING**WARNING**

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

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

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

WARNINGWARNING**WARNING**

Example of Public Web Page and Other Banners

Legal Notices for DEPARTMENT OF HEALTH AND HUMAN SERVICES
Publicly Accessible Web Sites

1. PRIVACY NOTICE

If you visit our site to read or download information, we collect and store only the following information about you: the name of the domain from which you access the Internet, the date and time you access our site, and the Internet address of the Web site from which you linked directly to our site. We will not obtain personally identifying information about you when you visit our site unless you voluntarily choose to provide such information to us by e-mail or you complete a comment form, forum registration site, or other online form. The Department of Health and Human Services does not give, sell, or transfer personal information to third parties unless required by law, such as the Freedom of Information Act. For site management, information is collected for statistical purposes. Computer software programs are used to create summary statistics about visits to Department of Health and Human Services Web sites, which are used for such purposes as assessing what information is of most and least interest, determining technical design specifications, and identifying system performance or problem areas. No information subject to the Privacy Act, such as name and address, is collected or used for this analysis. Raw data logs are used for no other purposes and are scheduled for regular destruction in accordance with National Archives and Records Administration Guidance. Except for authorized law-enforcement investigations, no other attempts are made to identify individual users or their usage habits. The Department of Health and Human Services Web sites do not, as a rule, enable “cookies.” One or more Department of Health and Human Services Operating Divisions may use cookies. For additional information specific to a Department of Health and Human Services Operating Division regarding their use and other privacy information, please visit that Operating Division’s Web site. Generally, individuals are strongly discouraged from sending any personal information, such as a social security number (SSN), to the Department of Health and Human Services Web master or any Department of Health and Human Services e-mail address. It may be necessary on certain Operating Division Web sites to collect personally identifiable information (name, e-mail address, SSN, or other unique identifier) but only if you specifically and knowingly provide it. Personally identifying information you provide will be used only for such other purposes as are described at the point of collection by the Operating Division asking for the information.

2. NOTICE OF MONITORING

You are entering an Official United States Government System, which may be used only for authorized purposes. The Government may monitor and audit usage of this system, and all persons are hereby notified that use of this system constitutes consent to such monitoring and auditing. Unauthorized attempts to upload information and/or change information on these Web sites are strictly prohibited and are subject to prosecution under the Computer Fraud and Abuse Act of 1986 and 18 U.S.C. §§1001 and 1030.

3. DISCLAIMER OF ENDORSEMENT

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

4. DISCLAIMER OF LIABILITY

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

5. COPYRIGHT STATUS

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

6. OFFICIAL SEAL, NAMES, AND SYMBOLS

Federal law prohibits use of any symbol, emblem, seal, insignia, or badge of any entity of the Department of Health and Human Services or any colorable imitation of such words, initials, symbols, emblems, or seals in connection with any advertisement, solicitation, business activity, or product where such use could reasonably be interpreted as conveying the false impression that such advertisement, solicitation, business activity, or product is in any manner approved, endorsed, sponsored, or authorized by, or associated with, the Department of Health and Human Services.

Appendix L: Services Blocked Using the Firewall

Application	Port No.	Action
Login services	telnet – 23/tcp	Restrict w/ strong authentication
	SSH – 22/tcp	Restrict to specific systems
	FTP – 21/tcp	Restrict w/ strong authentication
	NetBIOS – 139/tcp	Always block
	r services – 512/tcp – 514/tcp	Always block
RPC and NFS	Portmap/rpcbind –111/tcp/udp	Always block
	NFS – 2049/tcp/udp	Always block
	Lockd – 4045/tcp/udp	Always block
NetBIOS in Windows NT	135/tcp/udp	Always block
	137/udp	Always block
	138/udp	Always block
	139/tcp	Always block
	445/tcp/udp in Windows 2000	Always block
X Windows	6000/tcp – 6255/tcp	Always block
Naming Services	DNS – 53/udp	Restrict to external DNS servers
	DNS zone transfers – 53/tcp	Block unless external secondary
	LDAP – 389/tcp/udp	Always block
Mail	SMTP – 25/tcp	Block unless external mail relays
	POP – 109/tcp and 110/tcp	Always block
	IMAP – 143/tcp	Always block
Web	HTTP – 80/tcp and SSL – 443/tcp	Block unless to public Web servers
	May also want to block common high-order HTTP port choices – 8000/tcp, 8080/tcp, 8888/tcp, etc.	
"Small Services"	Ports Below 20/tcp/udp	Always block
	Time – 37/tcp/udp	Always block

Application	Port No.	Action
Miscellaneous	TFTP – 69/udp	Always block
	Finger – 79/tcp	Always block
	NNTP – 119/tcp	Always block
	NTP – 123/tcp	Always block
	LPD – 515/tcp	Always block
	Syslog – 514/udp	Always block
	SNMP – 161/tcp/udp, 162/tcp/udp	Always block
	BGP – 179/tcp	Always block
	SOCKS – 1080/tcp	Always block
ICMP	Block incoming echo request (ping and Windows trace route).	
	Block outgoing echo replies, time exceeded, and destination unreachable messages except “packet too big” messages (type 3, code 4). This item assumes that you are willing to forego the legitimate uses of ICMP echo request to block some known malicious uses.	