



































































































## Appendix D: Glossary

---

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

**Critical Infrastructure Protection (CIP)** — those physical and cyber-based systems essential to the minimum operations of the economy and government. They include, but are not limited to, telecommunications, energy, banking and finance, transportation, water systems, and emergency services, both governmental and private.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

**Information Technology** — any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by an executive agency. Equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment, or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources (Defined in 40 U.S.C., SEC. 1401).

**IT Investments** — IT resources that are implemented to strengthen and improve the organization's strategic objectives and business plans while reducing cost.

**Integrity** — guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity (Defined in 44 U.S.C., § 3542).

**Intranet** — an internal network intended for HHS only use.

**Label** — marking an item of information to reflect its security classification.

(a) Internal Label. Marking an item of information to reflect the classification of the information within the confines of the medium containing the information.

(b) External Label. The visible and readable marking on the outside or cover of the medium that reflects the classification of the information resident within the medium.

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

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

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

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

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

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

**Need to Know** — the necessity for access to or knowledge of or possession of specific information required to carry out official duties.

**Network** — comprises communications media and all components attached thereto whose responsibility is the transfer of information among a collection of IT systems or workstations. Network components include packet switches, front-end computers, network controllers, technical control devices, and other networks. In the context of this manual, such networks are: (a) under the operational control of an HHS official, (b) used for the transmission of classified or SBU data, and (c) may provide connectivity among information systems operated by various classified or SBU information components. Networks include wide- and local-area technologies.

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

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

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

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

**Personnel Security Clearance** — an administrative determination that an individual is eligible from a security point of view for access to classified information of the same or lower category as the level of the personnel security clearance being granted.

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

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

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

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

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

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

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

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

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

**Rules of Behavior** — the rules that have been established and implemented concerning use of, and security in, the system. Rules will clearly delineate responsibilities and expected behavior of all individuals with access to the system. Rules should cover such matters as work at home, dial-in access, connection to the Internet, use of copyrighted works, unofficial use of federal government equipment, assignment and limitation of system privileges, and individual accountability (Defined in NIST SP 800-18, Appendix D).

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

**Scan** — to examine computer coding and programs sequentially, part by part. For viruses, scans are made for virus signatures or potentially unsafe practices (e.g., changes to an executable file, direct writes to specific disk sectors).

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

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

**Security Safeguards** — the protective measures and controls prescribed to meet the security requirements specified for an IT system. Safeguards may include, but are not necessarily limited to, hardware and software security features; operation procedures; accountability procedures; access and distribution controls; management constraints; personnel security; and physical structures, areas, and devices.

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

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

**Sensitivity** — the IT environment consists of the system, data, and applications that must be examined individually and in total. All systems and applications require some level of protection for confidentiality, integrity, and/or availability; these levels of required protection are determined by an evaluation of the sensitivity of the information processed, the relationship of the system to the organization's mission, and the economic value of the system components.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

## Appendix E: Information Security Program Documents

---

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

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

# Appendix F: Departmental Policy Waiver

## Departmental Policy Waiver

Date: \_\_\_\_\_

Agency Name: \_\_\_\_\_

Agency Requester Name: \_\_\_\_\_

Phone Number: \_\_\_\_\_

Departmental Policy: \_\_\_\_\_

Justification for noncompliance or deviation: \_\_\_\_\_

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

\_\_\_\_\_  
Agency Representative Signature

\_\_\_\_\_  
Date

\_\_\_\_\_  
Agency Chief Security Officer (CSO)

\_\_\_\_\_  
Date

## Acknowledgements

---

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