CENTERS for MEDICARE & MEDICAID SERVICES
Enterprise Information Security Group
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Risk Management Handbook
Volume I
Chapter 10

CMS Risk Management Terms, Definitions, and Acronyms

FINAL
Version 1.0
July 13, 2012

Document Number: CMS-CISO-2012-vI-ch10

(This Page Intentionally Blank)

SUMMARY OF CHANGES IN *CMS RISK MANAGEMENT TERMS, DEFINITIONS, AND ACRONYMS,* VERSION 1.0

1. Baseline Version.

Risk Management Handbook Volume I Chapter 10, *CMS Risk Management Terms, Definitions, and Acronyms*, supersedes *CMS Information Security Terms, Definitions, and Acronyms* Version 4.00, dated March 8, 2009.

(This Page Intentionally Blank)

TABLE OF CONTENTS

(This Page Intentionally Blank)

1 INTRODUCTION

The *CMS Risk Management Terms, Definitions, and Acronyms* provides definitions and acronyms for common terms in information system risk management, including information security. Terms and acronyms are listed in alphabetical order together with the definition that applies within CMS. When CMS is not the primary term/definition source, the source is enclosed in brackets ("[ ]") after the definition. Acronyms for sources are explained in the acronyms list in section 1.2.

Some terms and acronyms may have multiple definitions depending on their context. When multiple term/acronym definitions are provided, there is no hierarchy or importance placed on the order or numerical value of the definition.

1.1 TERMS AND DEFINITIONS

The alphabetical tables of CMS risk management terms and definitions begin on page 2 of this document.

1.1.1 A

Term	Definition
Acceptable Level of Risk	The tolerable level of risk that is determined from: an analysis of threats and vulnerabilities; the sensitivity of data and applications; a cost/ benefit analysis; and a study of the technical and operational feasibility of available controls.
Acceptance	The act of an authorized representative of the government by which the government, for itself or as agent of another, assumes control or ownership of existing identified supplies tendered or approves specific services rendered as partial or complete performance of the contract. It is the final determination whether or not a facility or system meets the specified technical and performance standards. [NIST SP 800-64]
Access	1. The ability or the means necessary to “read”, “write”, modify or communicate data or otherwise make use of any system resource. 2. A specific type of interaction between a subject and an object that results in the flow of information from one to the other. [NCSC-TG-004] 3. Opportunity to make use of an information system resource. [CNSSI 4009]
Access Control	1. Limiting access to information system resources only to authorized users, programs, processes, or other systems. [CNSSI 4009] 2. The process of granting or denying specific requests: 3. Obtain and use information and related information processing services; and 4. Enter specific physical facilities (e.g., federal buildings, military establishments, border-crossing entrances). [FIPS 201; FISCAM]
Access Control List (ACL)	1. A register of: 2. Users (including groups, machines, processes) who have been given permission to use a particular system resource, and 3. The types of access they have been permitted. [NIST SP 800-12] 4. Mechanism implementing discretionary and/or mandatory access control between subjects and objects. [CNSSI 4009]
Access Control Mechanism	Security safeguard designed to detect and deny unauthorized access and permit authorized access in an information system. [CNSSI 4009]
Access Control Software	Software (e.g., CA-ACF2, RACF, CA-TOP SECRET), which is external to the operating system, provides a means of specifying who has access to a system, who has access to specific resources, and what capabilities authorized users are granted. Access control software can generally be implemented in different modes that provide varying degrees of protection such as denying access for which the user is not expressly authorized, allowing access which is not expressly authorized but providing a wanting, or allowing access to all resources without warning regardless of authority. [FISCAM]
Access Method	The technique used for selecting records in a file for processing, retrieval, or storage. [FISCAM]

Term	Definition
Access Path	1. Sequence of hardware and software components significant to access control. Any component capable of enforcing access restrictions or any component that could be used to bypass an access restriction should be considered part of the access path. 2. The path through which user requests travel, including the telecommunications software, transaction processing software, application program, etc. [FISCAM]
Access Privilege	Precise statements that define the extent to which an individual can access computer systems and use or modify the programs and data on the system, and under what circumstances this access will be allowed. [FISCAM]
Access Profile	Associates each user with a list of protected objects the user may access. [CNSSI 4009]
Access Script	A program or a series of encoded commands that enable a user to log-on to a system.
Access Type	Privilege to perform action on an object. Read, write, execute, append, modify, delete, and create are examples of access types. [CNSSI 4009]
Account Management	In network management, a set of functions that: (a) enables network service use to be measured and the costs of such use to be determined; and (b) includes all the resources consumed, the facilities used to collect accounting data, the facilities used to set billing parameters for the services used by customers, maintenance of the data bases used for billing purposes, and the preparation of resource usage and billing reports. Also, see User Account Management.
Accountability (See Non-repudiation)	1. 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 800-27A; FISCAM] 2. Process of tracing information system activities to a responsible source. [CNSSI 4009]
Accreditation	Obsolete (per 800-37 R1). See Authorization to Operate.
Acquisition	Includes all stages of the process of acquiring property or services, beginning with the process for determining the need for the property or services and ending with contract completion and closeout. [NIST SP 800-64]
Action Plan	An action plan is a record that indicates the methods by which one or more weaknesses are to be mitigated. An action plan contains milestones and projected completion dates, and is included in the Plan of Action and Milestones (POA&M) submission package and any POA&M reports.
Address of Record	The official location where an individual can be found. The address of record always includes the residential street address of an individual and may also include the mailing address of the individual. In very limited circumstances, an Army Post Office (APO) ox number, Fleet Post Office (FPO) box number or the street address of next-of-kin or of another contact individual can be used when a residential street address for the individual is not available.

Term	Definition
Adequate Security	Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information. [FIPS 200; OMB Circular A-130, App. III]
Adequately Met	Includes: • Functionality that performs correctly, • Sufficient protection against unintentional errors (by users or software), and • Sufficient resistance to intentional penetration or by-pass. [NIST SP 800-27A]
Administrative Access	An advanced level of access to a computer or application that includes the ability to perform significant configuration changes to the computer's operating system. Also referred to as "privileged access" or "root access." [NIST SP 800-40]
Administrative Safeguard	Administrative actions, policies, and procedures to manage the selection, development, implementation, and maintenance of security measures to protect electronic health information and to manage the conduct of the covered entity's workforce in relation to protecting that information. [HIPAA]
Advanced Encryption Standard (AES)	1. Specifies a U.S. Government-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. [NIST SP 800-46] 2. Through 2030, Triple Data Encryption Algorithm (TDEA) and FIPS 197 AES will coexist as FIPS-approved algorithms, thus allowing for a gradual transition to AES. [NIST SP 800-67]
Advisory	Notification of significant new trends or developments regarding the threat to the information system of an organization. This notification may include analytical insights into trends, intentions, technologies, or tactics of an adversary targeting information systems. [CNSSI 4009]
Agency	Any executive department, military department, government corporation, government-controlled corporation, or other establishment in the executive branch of the government (including the Executive Office of the President) or any independent regulatory agency, but does not include: 1) the General Accounting Office; 2) the Federal Election Commission; 3) the governments of the District of Columbia and of the territories and possessions of the United States and their various subdivisions; or 4) government-owned, contractor-operated facilities, including laboratories engaged in national defense research and production activities. Also referred to as Federal Agency. [FIPS 200; 44 USC Sec. 3502]
Alert	Notification that a specific attack has been directed at the information system of an organization. [CNSSI 4009]
Alternate Emergency Coordinator	A person who is trained to perform the duties of an Emergency Coordinator in the absence of the Primary Coordinator, or in case he/ she needs assistance.
Alternate Site	An operating location other than the one at which an activity is usually performed for use by business functions when the primary facilities are unavailable.

Term	Definition
Antivirus Software	A suite of applications that may be implemented to detect, identify, isolate and eradicate viruses, Trojan Horses, worms, and other forms of malicious code.
Application	1. Any program designed to perform a specific function directly for the user or, in some cases, for another application. Examples of applications include word processors; database programs; Web browsers; development tools; drawing, paint, and image editing programs; and communication programs. Applications use the services of the computer's operating system and other supporting programs. 2. Any data entry, update, query, or report program that processes data for the user. [NIST SP 800-40]
Application Control	Application controls are directly related to individual applications. They help ensure that transactions are valid, properly authorized, and completely and accurately processed and reported. [FISCAM]
Application Program	See Application.
Application Programmer	A person who develops and maintains application programs, as opposed to system programmers who develop and maintain the operating system and system utilities. [FISCAM]
Application Proxy Firewall	Software implemented on a server that acts as an intermediary between two computer systems engaged in communication. The application proxy firewall accepts service requests to and from client computers (computers placed behind and protected by the firewall), and makes the connection to a desired destination on behalf of the requesting party. As application proxy firewalls act on behalf of client computers, internal systems, and network structures are protected and hidden from public view. Application proxy firewalls differ from simple packet screening firewalls because they have the capability to view application layer data (web content, e-mail), and to make informed decisions based on packet content rather than simply packet headers.
Application Software	Software that is written to perform a specific business function (may include some commercial off-the-shelf [COTS] software).
Application System	A computer system written by or for a user that applies to the user's work; for example, a payroll system, inventory control system, or a statistical analysis system.
Approved (Algorithm or Cryptography)	FIPS-approved and/or NIST recommended. An algorithm or technique that meets at least one of the following: • Is specified in a FIPS or NIST Recommendation, • Is adopted in a FIPS or NIST Recommendation, or • Is specified in a list of NIST-approved security functions (e.g., specified as approved in the annexes of FIPS 140-2/3). [NIST SP 800-56B]
Architecture	A highly structured specification of an acceptable approach within a framework for solving a specific problem. An architecture contains descriptions of all the components of a selected, acceptable solution while allowing certain details of specific components to be variable to satisfy related constraints (e.g., costs, local environment, user acceptability, etc.). [FIPS 201]

Term	Definition
Archive	Information and records formatted for long-term storage for disaster recovery or other purposes. Items commonly archived include but are not limited to, magnetic media copies of operating system software, application software, and data and hardcopies of system records such as console logs, data listings, and software and firmware listings.
Arson	Any willful or malicious burning or attempt to burn, with or without intent to defraud, a dwelling house, public building, motor vehicle, personal property of another, etc.
Assertion	A statement from a verifier to a relying party that contains identity information about a subscriber. Assertions may also contain verified attributes. Assertions may be digitally signed objects or they may be obtained from a trusted source by a secure protocol.
Assessment and Authorization (A&A)	A collective reference, combining the two terms “Security Control Assessment” and “Authorization to Operate.”
Assessment Finding	Assessment results produced by the application of an assessment procedure to a security control or control enhancement to achieve an assessment objective; the execution of a determination statement within an assessment procedure by an assessor that results in either a satisfied or other than satisfied condition. [NIST SP 800-53A]
Assessment Method	A focused activity or action employed by an assessor for evaluating a particular attribute of a security control. [NIST SP 800-53]
Assessment Procedure	A set of activities or actions employed by an assessor to determine the extent to which a security control is implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. [NIST SP 800-53]
Asset	A major application, general support system, high impact program, physical plant, mission critical system, or a logically related group of systems. [NISTIR 7298]
Asset Evaluation	A quantitative and/or qualitative assessment to determine importance of the physical resources of the facilities, information, sensitivity of information, the operational impact of loss and/or denial of support, and the automated information systems resources providing that support.
Assurance	The 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: (a) functionality that performs correctly, (b) sufficient protection against unintentional errors (by users or software), and (c) sufficient resistance to intentional penetration or bypass. [NIST SP 800-30]
Asymmetric Keys	Two related keys, a public key and a private key that are used to perform complementary operations, such as encryption and decryption or signature generation and signature verification.

Term	Definition
Attack	1. The act of trying to bypass security controls on a system. An attack may be active, resulting in the alteration of data; or passive, resulting in the release of data. Note: The fact that an attack is made does not necessarily mean that it will succeed. The degree of success depends on the vulnerability of the system or activity and the effectiveness of existing countermeasures. [NCSC-TG-004] 2. Attempt to gain unauthorized access to an information system's services, resources, or information; or the attempt to compromise an information system's integrity, availability, or confidentiality. [CNSSI 4009]
Attacker	Party who is not the claimant or verifier but who wishes to execute the authentication protocol successfully as a claimant.
Audit	1. An activity to determine the adequacy of and adherence to established procedures, instructions, specifications, codes and standards, or other applicable contractual and licensing requirements and effectiveness of implementation. (Most common forms of audits are compliance, operational or vulnerability). 2. An independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures. [NIST SP 800-32; CNSSI 4009]
Audit Data	Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event. [NIST SP 800-32]
Audit Reduction Tool	Preprocessors designed to reduce the volume of audit records to facilitate manual review. Before a security review, these tools can remove many audit records known to have little security significance. These tools generally remove records generated by specified classes of events, such as records generated by nightly backups. [NIST SP 800-12]
Audit Software	Generic audit software consists of a special program or set of programs designed to audit data stored on computer media. Audit software performs functions such as data extraction and reformatting, file creation, sorting, and downloading. This type of audit software may also be used to perform computations, data analysis, sample selection, summarization, file stratification, field comparison, file matching, or statistical analysis. The term audit software may also refer to programs that audit specific functions, features, and controls associated with specific types of computer systems to evaluate integrity and identify security exposures. [FISCAM]
Audit Trail	1. A record showing who has accessed a computer system and what operations he/she has performed during a given period of time. These recordings must enable the re-creation, review, and examination of all events surrounding counter-policy activities within the system. 2. Chronological record of system activities to enable the reconstruction and examination of the sequence of events and/or changes in an event. [CNSSI 4009; FISCAM]

Term	Definition
Authenticate	To confirm the identity of an entity when that identity is presented. [NIST SP 800-32]
Authentication	1. Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system. [FIPS 200] 2. The corroboration that a person is the one claimed. [HIPAA]
Authentication Mechanism	Hardware or software-based mechanisms that force users to prove their identity before accessing data on a device. [NIST SP 800-72]
Authentication Protocol	A well-specified message exchange process that verifies possession of a token to authenticate a claimant remotely. Some authentication protocols also generate cryptographic keys that are used to protect an entire session, so that the data transferred in the session is protected. [NIST SP 800-63]
Authenticity	The quality of data integrity that originates from its purported source.
Authorization	The acceptance that a requestor has permission to access a resource. Also see Security Authorization (to Operate).
Authorization to Operate (ATO)	The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls. [NIST SP 800-37 R1]
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. [FIPS 200]
Automated Information Security	See System Security.
Automated Information System (AIS)	1. An assembly of computer hardware, software and/or firmware that is configured to collect, create, communicate, compute, disseminate, process, store, and/or control data or information. 2. The organized collection, processing, transmission, and dissemination of automated information in accordance with defined procedures. [OMB Circular A-130]
Automated Labeling	Refers to labels employed on internal data structures (e.g., records, files) within the information system. [NIST SP 800-53]
Automated Marking	Refers to markings employed on external media (e.g., hardcopy documents output from the information system). The markings used in external marking are distinguished from the labels used on internal data structures described in automated labeling. [NIST SP 800-53]
Automated System	A configuration of hardware and software infrastructure, applications, and associated documentation, either custom designed or commercial off-the-shelf (COTS) software, or combination thereof, that automates the activities of collecting and/or accessing data or information and performing logical computations in support of CMS' processes.
Availability	The property that data or information is accessible and usable upon demand by an authorized person. [HIPAA]

Term	Definition
Awareness (Information Security)	1. 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. [NIST SP 800-16] 2. Activities which seek to focus an individual's attention on an (information security) issue or set of issues. [NIST SP 800-50] Also see Training (Information Security).

1.1.2 B

Term	Definition
Back Office Function	An office, building, or function that is used by an organization to conduct support activities.
Background Investigation (BI)	This is a more in-depth version of the Limited Background Investigation (LBI) since the personal investigation coverage is the most recent five to seven years. This investigation is required of those going into the highest risk public trust positions (Level 6). [DHHS *Personnel Security/Suitability Handbook*]
Backup	1. A backup is a copy of data. This copy is a safeguard against unexpected data loss and application errors; should original data be lost, the backup can be installed to make it available again. 2. Any duplicate of a primary resource function, such as a copy of a computer program or data file. This standby is used in case of loss or failure of the primary resource. [FISCAM]
Backup and Recovery Test	A test to verify that a system can be re-established after a failure. This is accomplished by returning to a point in the processing cycle before any errors or loss occurred and reprocessing subsequent transactions.
Backup Plan	See Contingency Plan (CP).
Backup Procedure	Regular maintenance procedure that copies all new or altered files to a backup storage medium, such as a tape drive. [FISCAM]
Baseline	1. Configuration identification formally designated and applicable at a specific point in the life cycle of a configuration item. 2. Specification or product that has been formally reviewed and agreed upon, that thereafter serves as the basis for further development, and that can be changed only through formal change control procedures. [IEEE Std. 610-12-1990] 3. Document or a set of such documents formally designated and fixed at a specific time during the life cycle of a configuration item. [IEEE Std. 610-12-1990] 4. Any agreement or result designated and fixed at a given time, from which changes require justification and approval. [IEEE Std. 610-12-1990]

Term	Definition
Baseline Configuration	Includes information about a particular component's makeup (e.g., the standard software load for a workstation or notebook computer including updated patch information) and the component's logical placement within the information system architecture. Also includes a well-defined and documented specification to which the information system is built and deviations, if required, are documented in support of mission needs/objectives. [NIST SP 800-53]
Basic Input/Output System (BIOS)	The basic program that handles instructions, and interfaces to initialize and operate input and output procedures for computer hardware.
Batch (Processing)	A mode of operation in which transactions are accumulated over a period of time, such as a day, week, or month and then processed in a single run. In batch processing, users do not interact with the system while their programs and data are processing as they do during interactive processing. [FISCAM]
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. [GAO Assessing Risks and Returns: A Guide for Evaluation Agencies' IT Investment Decision-making]
Biometric	A measurable, physical characteristic or personal behavioral trait used to recognize the identity, or verify the claimed identity, of an applicant. Facial images, fingerprints, and handwriting samples are all examples of biometrics. [FIPS 201]
Biometric Authentication	1. The verification of an individual identity based on a unique and measurable physical characteristic, such as a fingerprint. 2. The process of verifying or recognizing the identity of a person based on physiological or behavioral characteristics. Biometric devices include fingerprints, retina patterns, hand geometry, speech patterns, and keystroke dynamics. [FISCAM]
Biometric Information	The stored electronic information pertaining to a biometric. This information can be in terms of raw or compressed pixels or in terms of some characteristic (e.g., patterns). [FIPS 201]
Bit	A binary digit: 0 or 1.
Bluetooth	A wireless protocol developed as a cable replacement to allow equipped devices to communicate with each other within a short distance. [NIST SP 800-124]
Boundary Protection	Monitoring and control of communications at the external boundary between information systems completely under the management and control of the organization and information systems not completely under the management and control of the organization, and at key internal boundaries between information systems completely under the management and control of the organization, to prevent and detect malicious and other unauthorized communication, employing controlled interfaces (e.g., proxies, gateways, routers, firewalls, encrypted tunnels). [NIST SP 800-53]

Term	Definition
Boundary Protection Device	A device with appropriate mechanisms that: (i) facilitates the adjudication of different interconnected system security policies (e.g., controlling the flow of information into or out of an interconnected system); and/or (ii) monitors and controls communications at the external boundary of an information system to prevent and detect malicious and other unauthorized communications. Boundary protection devices include such components as proxies, gateways, routers, firewalls, guards, and encrypted tunnels. [NIST SP 800-39]
Breach	1. The circumvention of some element of computer security, with or without detection, which could result in a penetration of the affected computer's software or databases, another device or the network to which the affected computer may be connected. 2. Includes the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to personally identifiable information, whether physical or electronic. [OMB M-07-16]
Browsing	1. The act of electronically perusing files and records without authorization. [FISCAM] 2. The act of searching through storage to locate or acquire information without necessarily knowing of the existence or the format of the information being sought. [CNSSI 4009]
Buffer Overflow	The act of introducing arbitrary code executed on a system, which does not adequately check input for appropriate length.
Build	An operational version of a system or component that incorporates a specified subset of the capabilities that the final product will provide. [IEEE Std. 610-12-1990]
Business Case Analysis (BCA)	The analysis establishes sound business reasons for proceeding with a project by providing insight into how the project supports business needs and the strategic goals of CMS. The BCA describes how the project aligns with CMS's Information Technology Architecture and identifies the project's assumptions and constraints. The BCA identifies the gap between current capability and new business needs, discusses alternatives for accomplishing the project, contains a cost/ benefit analysis that is consistent with the preferred alternative, and presents a high-level logical design. The design verifies that the proposed solution will be compatible with the CMS architecture and begins to establish the impact of the project on the infrastructure. The BCA next provides an assessment of business risks, describes the acquisition strategy, and outlines the project plan. Finally, an appendix containing the documented and validated user and system requirements shall be included. Additional details of the alternatives analysis may also be included as an appendix, if necessary.
Business Continuity and Contingency Plan (BCCP)	A plan for emergency response, backup operations, and post-disaster recovery maintained as a part of the subject's program that will ensure the availability of critical resources and facilitate continuity of operations in emergencies.

Term	Definition
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. [NIST SP 800-34]
Business Impact Analysis (BIA)	1. The process of analyzing current and planned business functions and the effect that their interruption in service may have on the organization. 2. An analysis of an information technology system's requirements, processes, and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption. [NIST SP 800-34]
Business Owner	1. The entity or entities responsible for defining, promoting, endorsing, and upholding the business needs and user requirements for the system, and for performing user acceptance testing of the final product(s) based on those business needs and user requirements. The Business Owner/Partner defines and validates system functionality, access rights, business rules, and the privacy classification, timeliness, completeness, and accuracy of data. 2. The individual who is responsible for making and communicating judgments and decisions on behalf of the organization with regard to the use, identification, classification, and protection of a specific information asset. 3. Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system. [FIPS 200; NIST SP 800-53A]
Business Partner	1. Non-federal personnel who perform services for the federal government at a site owned by the partner under the terms and conditions of a contractual agreement. Business Partners need security training commensurate with their responsibilities for performing work under the terms and conditions of their contractual agreements. 2. Business Partners include Medicare carriers, Fiscal Intermediaries, Common Working File host sites, standard claims processing system maintainers, regional laboratory carriers, claims processing data centers, Medicare Administrative Contractors (MACs) (including Durable Medical Equipment Medicare Administrative Contractors [DMEMAC] and A/B Medicare Administrative Contractors [ABMAC]) and Enterprise Data Centers (EDCs).
Business Recovery/ Resumption Plan (BRP)	The documentation of a predetermined set of instructions or procedures that describe how business processes will be restored after a significant disruption has occurred. [NIST SP 800-34] Also see Disaster Recovery Plan (DRP).

1.1.3 C

Term	Definition
Certificate	Security information signed electronically by an authority and used as identification. Certificates are generally signed using public key technology.

Term	Definition
Certificate Policy	A specialized form of administrative policy tuned to electronic transactions performed during certificate management. It addresses all aspects associated with the generation, production, distribution, accounting, compromise, recovery, and administration of digital certificates. Indirectly, a certificate policy can also govern the transactions conducted using a communications system protected by a certificate-based security system. By controlling critical certificate extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications. [NIST SP 800-32]
Certificate Revocation List (CRL)	A list of revoked public key certificates created and signed digitally by a Certification Authority. See [RFC 3280].
Certification	The process of verifying the correctness of a statement or claim and issuing a certificate as to its correctness. [FIPS 201]
Certification Agent	Obsolete (per 800-37 R1). See Security Control Assessor.
Certification and Accreditation (C&A)	Obsolete (per 800-37 R1). Note: This term and definition are superseded by Assessment and Authorization (A&A).
Certification Authority (CA)	A trusted entity that issues and revokes public key certificates. [FIPS 201]
Certification Practice Statement (CPS)	A statement of the practices that a Certification Authority employs in issuing, suspending, revoking and renewing certificates and providing access to them, in accordance with specific requirements (i.e., requirements specified in this Certificate Policy, or requirements specified in a contract for services). [NIST SP 800-32]
Chain of Custody	A process that tracks the movement of evidence through its collection, safeguarding, and analysis lifecycle by documenting each person who handled the evidence, the date/time it was collected or transferred, and the purpose for the transfer. [NIST SP 800-72]
Challenge Response Protocol	An authentication protocol where the verifier sends the claimant a challenge (usually a random value or a nonce) that the claimant combines with a shared secret (often by hashing the challenge and secret together) to generate a response that is sent to the verifier. The verifier knows the shared secret and independently can compute the response and compare it with the response generated by the claimant. If the two are the same, the claimant is considered to have authenticated himself successfully. When the shared secret is a cryptographic key, such protocols are generally secure against eavesdroppers. When the shared secret is a password, an eavesdropper does not intercept the password itself directly, but the eavesdropper may be able to find the password with an off-line password guessing attack.
Change Request	A request to modify any aspect of a system or environment including baseline requirements, hardware, or software.
Checkpoint	The process of saving the current state of a program and its data, including intermediate results to disk or other non-volatile storage, so that interrupted programs could be restarted at the point at which the last checkpoint occurred. [FISCAM]

Term	Definition
Chief Information Officer (CIO)	1. Agency official responsible for: • Providing advice and other assistance to the head of the executive agency and other senior management personnel of the agency to ensure that information technology is acquired and information resources are managed in a manner that is consistent with laws, Executive Orders, directives, policies, regulations, and priorities established by the head of the agency; • Developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture for the agency; and • Promoting the effective and efficient design and operation of all major information resources management processes for the agency, including improvements to work processes of the agency. [FIPS 200; P.L. 104-106, Sec. 5125(b)] 2. The incumbent in the position entitled Chief Information Officer.
Chief Information Security Officer (CISO)	The incumbent in the position entitled Chief Information Security Officer.
Cipher Key Lock	A lock with a key pad-like device that requires the manual entry of a predetermined code for entry. [FISCAM]
Cipher Text (or Ciphertext)	Data output from the cipher or input to the inverse cipher. Data in its encrypted form. [FISCAM]
Claimant	A party whose identity is to be verified using an authentication protocol.
Classified Data	Data that requires safeguarding in the interest of national security. [CNSSI 4009]
Clear	To use software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also may include all addressable locations. [NIST SP 800-88]
Client (Application)	A system entity, usually a computer process acting on behalf of a human user, that makes use of a service provided by a server. [NIST SP 800-32]
Clinger-Cohen Act of 1996	Also known as Information Technology Management Reform Act. A statute that substantially revised the way that information technology (IT) resources are managed and procured, including a requirement that each agency design and implement a process for maximizing the value and assessing and managing the risks of IT investments. [NIST SP 800-64]

Term	Definition
Cloud Computing	A model for enabling on-demand network access to a shared pool of configurable IT capabilities/resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. It allows users to access technology-based services from the network cloud without knowledge of, expertise with, or control over the technology infrastructure that supports them. This cloud model is composed of five essential characteristics (on-demand self-service, ubiquitous network access, location independent resource pooling, rapid elasticity, and measured service); three service delivery models (Cloud Software as a Service [SaaS], Cloud Platform as a Service [PaaS], and Cloud Infrastructure as a Service [IaaS]); and four models for enterprise access (Private cloud, Community cloud, Public cloud, and Hybrid cloud). Note: Both the user's data and essential security services may reside in and be managed within the network cloud. [NIST IR 7298]
Code	Instructions written in a computer programming language. [FISCAM] Also see Object Code and Source Code.
Cold Site	1. A disaster recovery facility that provides office space, but no machinery. The site has to be supplied with its own computers and other equipment in order to continue operations. 2. 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. [NIST SP 800-34; FISCAM]
Collaborative Computing	Applications and technology (e.g., white boarding, group conferencing) that allow two or more individuals to share information real time in an inter- or intra-enterprise environment. [CNSSI 4009]
Command	A job control statement or a message, sent to the computer system, that initiates a processing task. [FISCAM]
Commercial Off-the-Shelf (COTS)	Software and hardware that already exists and is available from commercial sources. It is also referred to as off-the-shelf. [NIST SP 800-64]
Common Control	A security control that is inherited by one or more organizational information systems. [NIST SP 800-37 R1]
Common Control Provider (CCP)	An organizational official responsible for the development, implementation, assessment, and monitoring of common controls (i.e., security controls inherited by information systems). {NIST SP 800-37 R1]
Common Vulnerabilities and Exposures (CVE)	A dictionary of common names for publicly known information technology system vulnerabilities. [NIST SP 800-51]
Communications Program	A program that enables a computer to connect with another computer and exchange information by transmitting or receiving data over telecommunications networks. [FISCAM]

Term	Definition
Communications Security (COMSEC)	Security controls in place to ensure that data transmission is protected from eavesdropping and message tampering. The information transmitted can be authenticated via strong cryptography and the exchange of strong encryption key information to protect all information from unauthorized users. [CNSSI 4009]
Compact Disc Read-Only Memory (CD-ROM)	A form of optical rather than magnetic storage. CD-ROM devices are generally "read-only". [FISCAM]
Compatibility	1. The ability of two or more systems or components seamlessly to perform required services. 2. The capability of a computer, device, or program to function with or substitute for another make and model of computer, device, or program. Also, the capability of one computer to run the software written to run on another computer. Standard interfaces, languages, protocols, and data formats are key to achieving compatibility. [FISCAM]
Compensating Control	The management, operational, and technical controls (i.e., safeguards or countermeasures) employed by an organization in lieu of the recommended controls in the low, moderate, or high security control baselines, that provide equivalent or comparable protection for an information system. [FIPS 200]
Compensating Security Control	The management, operational, and technical controls (i.e., safeguards or countermeasures) employed by an organization in lieu of the recommended controls in the low, moderate, or high baselines described in NIST SP 800-53, that provide equivalent or comparable protection for an information system. [NIST SP 800-53]
Complexity	The degree of intricacy of a system or system component, determined by such factors as the number of conditional branches, the degree of nesting and the length and types of data structures.
Component	A single resource with defined characteristics, such as a terminal or printer. These components are also defined by their relationship to other components. [FISCAM]
Compromise	Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred. [NIST SP 800-32]
Computer	See Computer System.
Computer Facility	A site or location with computer hardware where information processing is performed or where data from such sites are stored. [FISCAM]
Computer Forensics	The practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data. [NIST SP 800-61]
Computer Network	See Network.
Computer Operation	The function responsible for operating the computer and peripheral equipment, including providing the tape, disk, or paper resources as requested by the application systems. [FISCAM]
Computer Resource	See Resource.

Term	Definition
Computer Room	Room within a facility that houses computers and/or telecommunication devices. [FISCAM]
Computer Security	The protection of a computer system or network against internal failure, human error, attack, and natural catastrophe with the goal of preventing improper disclosure, modification or destruction of information, or denial of service. See Information System Security and System Security.
Computer Security Incident	See Incident.
Computer Security Incident Response Capability (CSIRC)	That part of the computer security effort that provides the capability to respond to computer security threats rapidly and effectively. A CSIRC provides a way for users to report incidents, and it provides personnel and tools for investigating and resolving incidents, and mechanisms for disseminating incident-related information to management and users. Analysis of incidents also reveals vulnerabilities, which can be eliminated to prevent future incidents. [NIST SP 800-3]
Computer Security Incident Response Team (CSIRT)	A capability set up for assisting in responding to computer security-related incidents; also called a Computer Incident Response Team (CIRT) or a CIRC (Computer Incident Response Center, Computer Incident Response Capability). [NIST SP 800-61]
Computer System	1. A complete computer installation, including peripherals, in which all the components are designed to work with each other. [FISCAM] 2. Any equipment or interconnected system or subsystems of equipment used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information; including computers; ancillary equipment; software, firmware, and similar procedures; services, including support services; and related resources as defined by regulations issued by the Administrator for General Services pursuant to section 111 of the Federal Property and Administrative Services Act of 1949. [Computer Security Act of 1987]
Computer-based Training (CBT)	A type of education in which the student learns by executing special training programs on a computer. Information security CBT is mandatory for users of CMS' information systems when an individual is initially issued their CMS User ID and then in conjunction with annual certification of their CMS User ID.
Computer-related Control	Computer-related controls help ensure the reliability, confidentiality, and availability of automated information. They include both general controls, which apply to all or a large segment of an entity's information systems, and application controls, which apply to individual applications. [FISCAM]
Confidentiality	1. The property that ensures that information is not made available or disclosed to unauthorized individuals, entities or processes; the degree to which sensitive data about individuals and organizations must be protected in accordance with the Privacy Act of 1974. 2. Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 USC Sec. 3542]

Term	Definition
Configuration	The arrangement or setup of a computer system, application, or component based upon system environment and organizational requirements.
Configuration (or Change) Control Board (CCB)	Group of people responsible for evaluating and approving or disapproving proposed changes to configuration items, and for ensuring implementation of approved changes. [IEEE Std. 610-12-1990]
Configuration Control	1. Process for controlling modifications to hardware, firmware, software, and documentation to protect the information system against improper modifications before, during, and after system implementation. [CNSSI 4009] 2. An element of configuration management, consisting of the evaluation, coordination, approval or disapproval, and implementation of changes to configuration items after formal establishment of their configuration identification. [IEEE Std. 610-12-1990]
Configuration Management (CM)	1. The process of identifying and defining the setup of an application or system, controlling changes to the system throughout the life-cycle, recording and reporting the status of the system and change requests, and verifying its completeness and correctness. 2. The control and documentation of changes made to a system's hardware, software, and documentation throughout the development and operational life of the system. [FISCAM]
Console	1. Console is a terminal attached to a minicomputer or mainframe and used to monitor the status of the system. It is also any display terminal for a computer. 2. Traditionally, a control unit such as a terminal through which a user communicates with a computer. In the mainframe environment, a console is the operator's station. [FISCAM]
Consortium	Currently consists of four CMS offices (Northeastern, Southern, Midwestern, and Western) that oversee the operations at the Regional Offices.
Consortium Contract Management Officer (CCMO)	Part of the Regional Consortiums, the CCMO is responsible for leading and directing contractor management at the consortium level.
Contingency Management	Establishing actions to be taken before, during and after an interruption in service.
Contingency Plan (CP)	1. A CP is a plan for emergency response, backup procedures, and post disaster recovery. Synonymous with disaster plan and emergency plan. 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. [NIST SP 800-34; FISCAM] 3. A plan for emergency response, backup procedures, and post-disaster recovery. Synonymous with disaster plan and emergency plan. [FIPS 11-3] Also see Business Continuity and Contingency Plan (BCCP).

Term	Definition
Contingency Planning	The process for ensuring, in advance, that any reasonable and foreseeable disruptions will have a minimal effect. Also see Contingency Plan (CP). [FISCAM]
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. [NIST SP 800-34]
Contracting Officer (CO)	A person with the authority to enter into, administer, and/or terminate contracts and make related determinations and findings. [NIST SP 800-64]
Contracting Officer's Technical Representative (COTR)	An individual to whom the contracting officer delegates certain contract administration responsibilities, usually related to technical direction and acceptance issues. [NIST SP 800-64]
Contractor	Non-federal personnel who perform services for the federal government under the terms and conditions of a contractual agreement. Contractors need security training commensurate with their responsibilities for performing work under the terms and conditions of their contractual agreements.
Control Techniques	Statements that provide a description of what physical, software, procedural or people related condition must be met or in existence in order to satisfy a core requirement.
Controlled Area	Any area or space for which the organization has confidence that the physical and procedural protections provided is sufficient to meet the requirements established for protecting the information and/or information system. [NIST SP 800-53A]
Controlled Interface	Mechanism that facilitates the adjudication of different interconnected system security policies (e.g., controlling the flow of information into or out of an interconnected system). [FIPS 200; CNSSI 4009]
Cookie	A piece of information supplied by a Web server to a browser, along with requested resource, for the browser to store temporarily and returns to the server on any subsequent visits or requests. [NIST SP 800-46]
Cost Determination	The value of efforts determined necessary to moderate identified risks. Cost factors may include labor, time, system response, and financial considerations.
Countermeasure	Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system. Synonymous with security controls and safeguards. [FIPS 200; CNSSI 4009]
Coverage	An attribute associated with an assessment method that addresses the scope or breadth of the assessment objects included in the assessment (e.g., types of objects to be assessed and the number of objects to be assessed by type). [NIST SP 800-53A]
Credential	An object that authoritatively binds an identity (and optionally, additional attributes) to a token possessed and controlled by a person. [NIST SP 800-63]
Credentials Service Provider (CSP)	A trusted entity that issues or registers subscriber tokens and issues electronic credentials to subscribers. The CSP may encompass Registration Authorities and verifiers that it operates. A CSP may be an independent third party, or may issue credentials for its own use.

Term	Definition
Credit Check	This is an automated credit record search conducted through various major credit bureaus. It is included in most background investigations except the basic National Agency Check and Inquiries (NACI) investigation required of employees entering Non-Sensitive (Level 1) positions. [DHHS *Personnel Security/Suitability Handbook*]
Crisis	A critical event that has the ability to affect dramatically an organization's profitability, reputation, or ability to operate.
Crisis Management	The overall coordination of an organization's response to a crisis in an effective, timely manner with the goal of avoiding or minimizing damage to the organization's profitability, reputation, or ability to operate.
Critical Asset	Those physical and information assets required for the performance of the site mission. [DHHS IRM Policy]
Critical Infrastructure	Systems and assets, whether physical or virtual, so vital to the U.S. that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. [42.USC 5195c(e)]
Criticality	The level of impact an interruption in service or exposure will have on an organization.
Criticality Level	Refers to the (consequences of) incorrect behavior of a system. The more serious the expected direct and indirect effects of incorrect behavior, the higher the criticality level. [NIST SP 800-60]
Cryptographic Algorithm	A well-defined computational procedure that takes variable inputs, including a cryptographic key, and produces an output. [FIPS 140-2]
Cryptographic Key (Key)	A parameter used in conjunction with a cryptographic algorithm that determines: • The transformation of plaintext data into ciphertext data, • The transformation of ciphertext data into plaintext data, • A digital signature computed from data, • The verification of a digital signature computed from data, • An authentication code computed from data, or • An exchange agreement of a shared secret. [FIPS 140-3]
Cryptographic Module	The set of hardware and/or software that implements approved security functions (including cryptographic algorithms and key generation) and are contained within the cryptographic boundary. [NIST SP 800-32; FIPS 140-3]
Cryptographic Strength	A measure of the expected number of operations required to defeat a cryptographic mechanism. [NIST SP 800-63]
Cryptographic Token	A token where the secret is a cryptographic key. [NIST SP 800-63]
Cryptography	1. The principles, means, and methods for rendering information unintelligible and for restoring encrypted information to intelligible form for an authorized party. 2. The discipline that embodies principles, means and methods for providing information security, including confidentiality, data integrity, non-repudiation, and authenticity. [NIST SP 800-21; FISCAM]

1.1.4 D

Term	Definition
Damage Assessment	Post-incident appraisal or determination of actual consequences to an organization including human, physical, economic, reputation and natural resource impacts.
Data	1. A representation of facts, concepts, or instructions in a manner suitable for communication, interpretation, or processing by human or electronic means. 2. Programs, files or other information stored in, or processed by, a computer system. [FIPS 112; FISCAM]
Data Administration	The function that plans for and administers the data used throughout the entity. This function is concerned with identifying, cataloging, controlling, and coordinating the information needs of the entity. [FISCAM]
Data Center	See Computer Facility.
Data Communications	1. The transfer of information from one computer to another through a communications medium, such as telephone lines, microwave relay, satellite link, or physical cable. [FISCAM] 2. The transfer of data between functional units by means of data transmission according to a protocol. [FIPS 11-3]
Data Contamination	1. The introduction of data of one sensitivity level into data of a lower or different sensitivity level. 2. An accidental or intentional violation of data integrity.
Data Control	The function responsible for seeing that all data necessary for processing is present and that all output is complete and distributed properly. This function is generally responsible for reconciling record counts and control totals submitted by users with similar counts and totals generated during processing. [FISCAM]
Data Dictionary	1. Contains a list of all files in the database, the number of records in each file, the names and types of each field, and authorization for access to each data element in the organization's files and databases. 2. A repository of information about data, such as its meaning, relationships to other data, origin, usage, and format. The dictionary assists company management, database administrators, systems analysts, and application programmers in effectively planning, controlling, and evaluating the collection, storage, and use of data. [FISCAM]
Data Element	A basic unit of information that has a unique meaning and subcategories (data items) of distinct value. Examples of data elements include gender, race, and geographic location. [NIST SP 800-47]
Data Encryption Algorithm (DEA)	The cryptographic engine that is used by the Triple Data Encryption Algorithm (TDEA). [NIST SP 800-67]

Term	Definition
Data Encryption Standard (DES)	1. The conversion of data into an unintelligible form so that it is readable except by authorized users is called data encryption. DES is an approved FIPS cryptographic algorithm that is compliant with FIPS 140-1 (DES is not approved under FIPS 140-2). 2. The NIST DES was adopted by the U.S. Government as FIPS 46 [at publication 46-1], which allows only hardware implementations of the data encryption algorithm. [FIPS 11-3] 3. The symmetric encryption algorithm that serves as the cryptographic engine for the Triple Data Encryption Algorithm (TDEA). [NIST SP 800-67] 4. The original "single" DES algorithm is no longer secure because it is now possible to try every possible key with special purpose equipment or a high performance cluster. [NIST SP 800-46]
Data File	See File.
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. [NIST SP 800-27A]
Data Owner	The individual who has the responsibility for making judgments and decisions on behalf of the organization with regard to the data's sensitivity/criticality level designation, its use, protection, and sharing.
Data Processing	1. The process whereby a computer and its programs organize/ manipulate data and the flow of data. 2. The computerized preparation of documents and the flow of data contained in these documents through the major steps of recording, classifying, and summarizing. [FISCAM]
Data Security	The protection of data from unauthorized (accidental or intentional) modification, destruction, or disclosure. [FIPS 39] Also see Security Management Function.
Data Validation	Checking transaction data for any errors or omissions that can be detected by examining the data. [FISCAM]
Database	1. A collection of interrelated data, often with controlled redundancy, organized according to a schema to serve one or more applications; the data are stored so that they can be used by different programs without concern for the data structure or organization. A common approach is used to add new data and to modify and retrieve existing data. [FIPS 11-3] 2. A collection of related information about a subject organized in a useful manner that provides a base or foundation for procedures, such as retrieving information, drawing conclusions, or making decisions. Any collection of information that serves these purposes qualifies as a database, even if the information is not stored on a computer. [FISCAM]
Database Administration (DBA) & Database Management (DBM)	Tasks related to creating, maintaining, organizing, and retrieving information from a database. [FISCAM]

Term	Definition
Database Administrator	The individual responsible for both the design of the database, including the structure and contents, and the access capabilities of application programs and users to the database. Additional responsibilities include operation, performance, integrity, and security of the database. [FISCAM]
Database Management System (DBMS)	1. A set of programs that control the organization, storage, and retrieval of data. The DBMS also controls the security and data integrity of the database. 2. A software product (DB2, IMS, IDMS) that aids in controlling and using the data needed by application programs. DBMSs organize data in a database, manage all requests for database actions, such as queries or updates from users, and permit centralized control of security and data integrity. [FISCAM]
Debug	To detect, locate, and correct logical or syntactical errors in a computer program. [FISCAM]
Degauss	To reduce the magnetic flux to virtual zero by applying a reverse magnetizing field. Also called demagnetizing. Degaussing any current generation hard disk (including but not limited to integrated drive electronics [IDE], enhanced integrated drive electronics [EIDE], advanced technology attachment [ATA], and small computer system interface [SCSI]) will render the drive permanently unusable since these drives store track location information on the hard drive in dedicated regions of the drive in between the data sectors. [NIST SP 800-88]
Demilitarized Zone (DMZ)	1. A small computer network that acts as a neutral area between an organization's internal private network and public networks. Firewall protection is usually implemented for the DMZ network, and an additional firewall layer protects the internal private network. A typical DMZ contains one or more servers intended for public access (web server, e-mail server, etc.), and prevents direct connections to the internal network from public, untrusted networks. 2. A network created by connecting two firewalls. Systems that are externally accessible but need some protections are usually located on DMZ networks. [NIST SP 800-41]
Denial of Service (DoS)	1. An action (or series of actions) that prevents any part of a system from functioning in accordance with its intended purpose. This includes any action that causes unauthorized destruction, modification, delay, or interruption of service. 2. An attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources. [NIST SP 800-61]
Depth	An attribute associated with an assessment method that addresses the rigor and level of detail associated with the application of the method. [NIST SP 800-53A]
Desktop Computer	Any personal computer or workstation used exclusively in a work environment at home or in the office, running a popular operating system, including Windows, Mac operating system (OS), and Linux. [NIST SP 800-124]

Term	Definition
Destruction	The result of actions taken to ensure that media cannot be reused as originally intended and that information is virtually impossible to recover or prohibitively expensive. [NIST SP 800-88]
Dial-up Access	1. A method of accessing a computer system remotely using telephone lines and a modem. 2. A means of connecting to another computer or a network like the Internet, over a telecommunications line using a modem-equipped computer. [FISCAM]
Dial-up Security Software	Software that controls access via remote dial-up. One method of preventing unauthorized users from accessing the system through an unapproved telephone line is through dial-back procedures in which the dial-up security software disconnects a call initiated from outside the network via dial-up lines, looks up the user's telephone number, and uses that number to call the user. [FISCAM]
Digital Signature	1. An electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a document, and possibly to ensure that the original content of the message or document that has been sent is unchanged. Digital signatures are easily transportable, cannot be imitated by someone else, and can be time-stamped automatically. The ability to ensure that the original signed message arrived means that the sender cannot easily repudiate it later. 2. The result of a cryptographic transformation of data which, when properly implemented, provides the services of: 3. Origin authentication, 4. Data integrity, and 5. Signer non-repudiation [FIPS 140-3]
Disaster	A sudden, unplanned, calamitous event that brings about damage or loss. Any unexpected or unexplained event that creates an organizational inability to provide critical business functions for a period of time.
Disaster Recovery	The response to an interruption in services by implementing a pre-determined process to restore an organization's business functions.
Disaster Recovery Plan (DRP)	1. The document or documents defining the resources, actions, tasks, and data required for restoring the business processes in the event of an interruption. 2. A written plan for processing critical applications in the event of a major hardware or software failure or destruction of facilities. [NIST SP 800-34]
Disclosure	Activities of employees that involve improper systems access and occasional disclosure of information found thereon, but not serious enough to warrant criminal prosecution. These cases should be entered on the Fraud Monitoring and Reporting System.
Discretionary Access Control (DAC)	The basis of this kind of security is that an individual user, or program operating on the user's behalf is allowed to specify explicitly the types of access other users (or programs executing on their behalf) may have to information under the user's control. [FIPS 191]

Term	Definition
Disk Storage	High-density random access magnetic storage devices that store billions of bits of data on round, flat plates that are either metal or plastic. [FISCAM]
Diskette	A removable and widely used data storage medium that uses a magnetically coated flexible disk of Mylar enclosed in a plastic case. [FISCAM]
Disposal	Disposal is the act of discarding media with no other sanitization considerations. This is most often done by paper recycling containing non-confidential information but may also include other media. [NIST SP 800-88]
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). [NIST SP 800-34]
Distributed Denial of Service (DDoS)	A denial of service (DoS) technique that uses numerous hosts to perform the attack. [NIST SP 800-61]
Domain	1. The scope of operations for an application or system. 2. A set of subjects, their information objects, and a common security policy. [NIST SP 800-27A]
Due Care	The responsibility that managers and their organizations have a duty to provide for information security to ensure that the type of control, the cost of control, and the deployment of control are appropriate for the system being managed. [NIST SP 800-30]

1.1.5 E

Term	Definition
e-Authentication	1. The process of establishing reasonable confidence in user identities presented electronically to an information system in order to conduct transactions. 2. The process of establishing confidence in user identities electronically presented to an information system. [NIST SP 800-63]
Eavesdropping	The action of unobserved listening to conversations between people or systems in order to obtain information.
Electronic Credential	Digital documents used in authentication that bind an identity or an attribute to a subscriber's token. [NIST SP 800-63]
Electronic Data Interchange (EDI)	A standard for the electronic exchange of business documents, such as invoices and purchase orders. EDI eliminates intermediate steps in processes that rely on the transmission of paper-based instructions and documents by performing them electronically, computer to computer. [FISCAM]
Electronic Evidence	Information and data of investigative value that is stored on or transmitted by an electronic device. [NIST SP 800-72]

Term	Definition
Electronic Mail (e-mail or email)	1. The transmission of memos and messages over a network. Within an enterprise, users can send e-mail to a single recipient or broadcast it to multiple users. With multi-tasking workstations, e-mail can be delivered and announced while the user is working in an application. Otherwise, e-mail is sent to a simulated mailbox in the network server or host computer, which must be interrogated. 2. A store and forward method of composing, sending, storing, and receiving messages over electronic communication systems. The term "email" (as a noun or verb) applies both to the Internet email system based on the simple mail transfer protocol (SMTP) and to X.400 systems, and to intranet systems allowing users within one organization to email each other. Often these workgroup collaboration organizations may use the Internet protocols or X.400 protocols for internal email service. Email is often used to deliver bulk unsolicited messages, or "spam", but filter programs exist which can automatically delete some or most of these, depending on the situation. [Wikipedia]
Electronic Media	1. General term that refers to media on which data are recorded via an electrically based process. [NIST SP 800-88] 2. Electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or transmission media used to exchange information already in electronic storage media (e.g., Internet, extranet, leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. [HIPAA]
Electronic Protected Health Information (EPHI)	Individually identifiable health information that is: • Transmitted by electronic media, or • Maintained in electronic media. [45 CFR Sec.160.103]
Electronic Signature	A symbol, generated by electronic means, that can be used to (i) identify the sender of information and (ii) ensure the integrity of the critical information received from the sender. An electronic signature may represent either an individual or an entity. Adequate electronic signatures are (i) unique to the signer, (ii) under the signer's sole control, (iii) capable of being verified, and (iv) linked to the data in such a manner that if data are changed, the signature is invalidated upon verification. Traditional user identification code/password techniques do not meet these criteria. [FISCAM]
E-mail Spoofing	Mail spoofing is the practice of changing the header that contains information regarding the originator, the addressee, and other recipients, so that the e-mail appears to come from somewhere or someone else.
Emergency Coordinator	The system member responsible for assessing emergency situations and making decisions to respond.
Encrypted Network	A network on which messages are encrypted (e.g., using Data Encryption Standard [DES], Advanced Encryption Standard [AES], or other appropriate algorithms) to prevent reading by unauthorized parties. [NIST SP 800-32]

Term	Definition
Encryption	1. The transformation of plain text (words) into cipher text (unintelligible) by cryptographic techniques in order to protect data from disclosure during network transmissions. 2. Conversion of plaintext to ciphertext using a cryptographic algorithm. [FIPS 185]
End Users	Employees who have access to computer systems and networks and process, store, or transmit information. This is the largest and most heterogeneous group of employees. It consists of everyone, from an executive with a desktop system to application programmers to data entry clerks.
Entity	1. Includes all CMS internal/external business organizations including their contractors/subcontractors, and organizational employees and facilities that support CMS business missions. 2. Either a subject (an active element that operates on information or the system state) or an object (a passive element that contains or receives information). [NIST SP 800-27A] 3. An individual (person), organization, device, or process. [NIST SP 800-57, Part 1]
Entropy	A measure of the amount of uncertainty that an attacker faces in determining the value of a secret. Entropy is usually stated in bits.
Environment	1. The state of a computer, usually determined by which programs are running and basic hardware and software characteristics that affect the development, operation, and maintenance of a system. 2. An aggregate of external procedures, conditions, and objects affecting the development, operation, and maintenance of an information system. [FIPS 200; CNSSI 4009]
Environment Control	This subset of physical access controls prevents or mitigates damage to facilities and interruptions in service. Smoke detectors, fire alarms and extinguishers, and uninterruptible power supplies are some examples of environmental controls. [FISCAM]
Environmental System Software	Software, which is required to operate the hardware equipment (sometimes referred to as operating system [OS] software) and software and utility programs that are used in the development of applications and/or databases (e.g., DB2, Oracle, Cobol, M204, and General Support System [GSS] commercial off-the-shelf [COTS] software).
Espionage	The covert act of spying through copying, reproducing, recording, photographing, interception etc. to obtain information through unauthorized means.
Evacuation	An organized withdrawal from a place or an area usually because of a crisis or emergency.
Event	Any observable occurrence in a network or system. [NIST SP 800-61]
Examine	A type of assessment method that is characterized by the process of checking, inspecting, reviewing, observing, studying, or analyzing one or more assessment objects to facilitate understanding, achieve clarification, or obtain evidence, the results of which are used to support the determination of security control effectiveness over time. [NIST SP 800-53A]

Term	Definition
Exception Criteria	Exception criteria refer to batch processes that return files or records as not meeting certain pre-defined criteria for processing.
Execute	A level of access that provides the ability to initiate a program. [FISCAM]
Exhibit 300	An annual document required by OMB, which refers to the requirements described in Section 300 of the OMB Circular A-11.
Exposure	The potential compromise associated with an attack exploiting a corresponding vulnerability.
External Connectivity	A computer or network connection to an outside, uncontrolled network that is unprotected by perimeter security. For example a modem connection to a network computer.
External Information System (or Component)	An information system or component of an information system that is outside of the accreditation boundary established by the organization and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness. [NIST SP 800-53A]
External Information System Service	An information system service that is implemented outside of the accreditation boundary of the organizational information system (i.e., a service that is used by, but not a part of, the organizational information system). [NIST SP 800-53A]
External Information System Service Provider	A provider of external information system services to an organization through a variety of consumer-producer relationships, including but not limited to: joint ventures; business partnerships; outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements); licensing agreements; and/or supply chain exchanges. [NIST SP 800-53A]
Extranet	A virtual network created by connecting two intranets. An organization that connects remote locations with a virtual private network (VPN) creates an extranet by linking its intranets together to form one virtual network. [NIST SP 800-41]

1.1.6 F

Term	Definition
Facility	A physical location containing the equipment, supplies, communication lines (voice and data), and related data necessary to perform transactions required under normal operating conditions. Also see Computer Facility.
False Positive	An alert that incorrectly indicates that malicious activity is occurring. [NIST SP 800-61]
Federal Acquisition Regulation (FAR)	The regulation that codifies uniform acquisition policies and procedures for executive agencies. [NIST SP 800-64]
Federal Enterprise Architecture (FEA)	A business-based framework developed by OMB to identify opportunities to simplify processes and unify work across the agencies and within the lines of business of the federal government in order to transform the federal government into one that is citizen-centered, customer-focused, results-oriented, and market-based and to maximize technology investments to better achieve mission outcomes.

Term	Definition
Federal Information Processing Standards (FIPS)	A standard for adoption and use by federal agencies that has been developed within the Information Technology Laboratory and published by the NIST, a part of the U.S. Department of Commerce. A FIPS covers some topic in information technology in order to achieve a common level of quality or some level of interoperability. [NIST SP 800-64]
Federal Information Security Management Act (FISMA)	Requires agencies to integrate information technology (IT) security into their capital planning and enterprise architecture processes at the agency, conduct annual IT security reviews of all programs and systems, and report the results of those reviews to the OMB. [NIST SP 800-65]
Federal Information System	An information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency. [40 USC Sec. 11331]
Federal Tax Information (FTI)	Generally, Federal Tax Returns and return information are confidential, as required by Internal Revenue Code (IRC) Section 6103. The information is used by the Internal Revenue Service (IRS) to ensure that agencies, bodies, and commissions are maintaining appropriate safeguards to protect the information confidentiality. [IRS 1075]
Field	A location in a record in which a particular type of data are stored. In a database, the smallest unit of data that can be named. A string of fields is a concatenated field or record. [FISCAM]
File	A collection of information logically grouped into a single entity and referenced by a unique name, such as a filename. [NIST SP 800-111]
File Descriptor Attack	The act of introducing non-negative integers that the system uses to keep track of files rather than using specific filenames.
File Encryption	The process of encrypting individual files on a storage medium and permitting access to the encrypted data only after proper authentication is provided. [NIST SP 800-111]
File Permissions	Access attributes associated with a file or directory, as defined in an access control list (ACL). Basic file permissions include the ability to “read”, “write”, and “execute”.
File Server	A computer used as a central repository for shared files and applications in a local area network (LAN) that can be accessed by other systems within the organization.
Filesystem (or File system)	A mechanism for naming, storing, organizing, and accessing files on logical volumes. [NIST SP 800-111]

Term	Definition
Firewall	1. Software and/or hardware deployed to maintain control over information going into and out of a network. 2. A firewall is a set of related programs, located at a network gateway that protects the resources of a private network from users from other networks. An enterprise with an intranet that allows its workers access to the wider Internet installs a firewall to prevent outsiders from accessing its own private data resources and for controlling what outside resources its own users have access to. 3. Hardware and software components that protect one set of system resources (e.g., computers, networks) from attack by outside network users (e.g., Internet users) by blocking and checking all incoming network traffic. Firewalls permit authorized users to access and transmit privileged information, and deny access to unauthorized users. [FISCAM]
Firmware	The programs and data components of a cryptographic module that are stored in hardware within the cryptographic boundary and cannot be dynamically written or modified during execution. [FIPS 140-2]
Folder	An organizational structure used by a file-system to group files. [NIST SP 800-111]
Folder Encryption	The process of encrypting individual folders on a storage medium and permitting access to the encrypted files within the folders only after proper authentication is provided. [NIST SP 800-111]
Fraud	A deception deliberately practiced to secure unfair or unlawful gain.
Full Disk Encryption	The process of encrypting all the data on the hard drive used to boot a computer, including the computer's operating system, and permitting access to the data only after successful authentication with the full disk encryption product. [NIST SP 800-111]

1.1.7 G

Term	Definition
Gateway	1. In a communications network, a network node equipped to interface with another network that uses different protocols. 2. In networks, a computer that connects two dissimilar local area networks, or connects a local area network (LAN) to a wide area network (WAN), minicomputer, or mainframe. A gateway may perform network protocol conversion and bandwidth conversion. [FISCAM]
General Control	The structure, policies, and procedures that apply to an entity's overall computer operations. They include an entity-wide security program, access controls, application development and change controls, and segregation of duties, system software controls, and service continuity controls. [FISCAM]

Term	Definition
General Support System (GSS)	1. Computer platform that incorporates hardware, operating system software, and environmental software to support major applications (e.g., data center, communications network). 2. An interconnected information resource, under the same direct management control, that shares common functionality. It normally includes hardware, software, information, data, applications, communications, facilities, and people. It provides support for a variety of users and/or applications. Individual applications supporting different business-related functions may run on a single GSS. Users may be from the same or different organizations. 3. An interconnected set of information resources, under the same direct management control, that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people. A system can be, for example, a local area network (LAN) including 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 shared information processing service organization. [OMB Circular A-130, App. III]
Generator	An independent source of electrical power usually fueled by diesel or natural gas.
Guessing Entropy	A measure of the difficulty that an attacker has in order to guess the average password used in a system. In this document, entropy is stated in bits. When a password has n-bits of guessing entropy then an attacker has as much difficulty guessing the average password as in guessing an n-bit random quantity. The attacker is assumed to know the actual password frequency distribution.
Guided Media	1. Those media in which a message flows through a physical media (e.g., twisted pair wire, coaxial cable). 2. Medium in which a message flows through a physical media (e.g., twisted pair wire, coaxial cable, optical fiber) providing a closed path between sender and receiver. [Computer Assisted Technology Transfer Laboratory, Oklahoma State University]
Guideline	Recommended security configurations, policies or actions developed to provide assistance in complying with one or more policies or standards.

1.1.8 H

Term	Definition
Hacker	An outside individual who attempts to access and/or compromise the confidentiality, integrity or availability of organizational data or systems.
Hacking	An unauthorized attempt to access and/or comprise a computer system and the data it contains.
Halon	A gas that does not damage computing equipment/machinery that is used to extinguish fires and is effective only in closed areas.
Handled	(As in “data handled.”) Stored, processed or used in an automated data processing (ADP) system or communicated, displayed, produced, or disseminated by an ADP system.

Term	Definition
Hardware	1. The physical part of a computer system including the machinery and equipment. 2. The physical components of information technology, including the computers, peripheral devices such as printers, disks, and scanners, and cables, switches, and other elements of the telecommunications infrastructure. [FISCAM]
Hash Function	A function that maps a bit string of arbitrary length to a fixed length bit string. Approved hash functions satisfy the following properties: (a) (One-way) It is computationally infeasible to find any input that maps to any pre-specified output, and (b) (Collision resistant) It is computationally infeasible to find any two distinct inputs that map to the same output.
Hash-based Message Authentication Code (HMAC)	A symmetric key authentication method using hash functions.
Hazardous Material	Any substance that poses a physical and/or health hazard. Health hazardous materials may be toxic, carcinogenic, corrosive, a sensitizer, or irritant. Physically hazardous materials may be flammable, explosive, unstable, water-reactive, an oxidizer, organic peroxide, combustible liquid or compressed gas.
High Impact System	An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of high. [FIPS 200]
Honeypot	A host that is designed to collect data on suspicious activity and has no authorized users other than its administrators.
Host-based Intrusion Detection System	IDSs that operate on information collected from within an individual computer system. [NIST SP 800-36]
Hot Site	1. An alternate facility that has the equipment and resources to recover the business functions affected in the event of a disaster. Hot-sites may vary in type of facilities offered (such as data processing, communication, or any other critical business functions needing duplication). 2. A fully operational off-site data processing facility equipped with both hardware and system software to be used in the event of a disaster. [NIST SP 800-34]
Hotfix	Microsoft's term for a security patch. [NIST SP 800-40] Also see Patch.
Hybrid Security Control	A security control that is implemented in an information system in part as a common control and in part as a system-specific control. [NIST SP 800-37 R1]

1.1.9 I

Term	Definition
Identification (ID)	1. The process of verifying the identity of a user, process, or device, usually as a prerequisite for granting access to resources in an information technology system. [NIST SP 800-47] 2. The process of discovering the true identity (i.e., origin, initial history) of a person or item from the entire collection of similar persons or items. [FIPS 201]
Identifier	A unique data string used as a key in the biometric system to name a person's identity and its associated attributes. [FIPS 201]
Identity	1. A unique name of an individual person. Since the legal names of persons are not necessarily unique, the identity of a person shall include sufficient additional information to make the complete name unique. [NIST SP 800-63] 2. The set of physical and behavioral characteristics by which an individual is uniquely recognizable. [FIPS 201]
Identity Proofing	The process by which a Customer Service Plan (CSP) and a Registration Authority validate sufficient, unique information to identify a person. [NIST SP 800-63]
Identity Verification	The process of confirming or denying that a claimed identity is correct by comparing the credentials (something you know, something you have, something you are) of a person requesting access with those previously proven and stored in the Personal Identity Verification (PIV) Card or system and associated with the identity being claimed. [NIST SP 800-79]
Identity-based Security Policy	A security policy based on the identities and/or attributes of the object (system resource) being accessed and of the subject (user, group of users, process, or device) requesting access. [NIST SP 800-33]
Image	An exact bit-stream copy of all electronic data on a device, performed in a manner that ensures the information is not altered. [NIST SP 800-72]
Impersonation	An attempt to gain access to a system by posing as an authorized user.
Implementation	The process of making a system operational in the organization. [FISCAM]
Implementation Standard	Specifies a CMS-assigned parameter, as mandated by NIST 800-53 (e.g., periodicity or value), or CMS specific amplification of how to implement the underlying *CMS Policy for the Information Security Program* (PISP) baseline requirement.
Inappropriate Usage	A person who violates acceptable use of any network or computer policies. [NIST SP 800-61]

Term	Definition
Incident	1. The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. It also means the loss of data through theft or device misplacement, loss or misplacement of hardcopy documents and misrouting of mail, all of which may have the potential to put the data at risk of unauthorized access, use, disclosure, modification, or destruction. 2. An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. [FIPS 200; NIST SP 800-53] 3. A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. [NIST SP 800-61]
Incident Handling	The mitigation of violations of security policies and recommended practices. [NIST SP 800-61]
Incident Response Plan	The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit the consequences of malicious cyber-attacks against an organization's information technology system(s). [NIST SP 800-34]
Incident Response Procedure	1. A formal process or set of procedures to be followed after notification of a suspected system's unauthorized action within a network or computer system. 2. Incident response involves detection, alert, triage, response (containment and eradication), recovery, and follow-up. The goal of a systematic approach to handle security incidents is to resume system and business operations as soon as possible while preserving the incident's forensics information for further analysis and security process enhancements.
Incineration	A physically destructive method of sanitizing media; the act of burning completely to ashes. [NIST SP 800-88]
Incremental Backup	The process of making a copy of only the files that have changed since the last backup instead of backing up every file.
Independent Security Assessor (or Team)	Any individual or group capable of conducting an impartial assessment of an organizational information system. Impartiality implies that the assessors are free from any perceived or actual conflicts of interest with respect to the developmental, operational, and/or management chain associated with the information system or to the determination of security control effectiveness. Independent security assessment services can be obtained from other elements within the organization or can be contracted to a public or private sector entity outside of the organization. Contracted assessment services are considered independent if the information system owner is not directly involved in the contracting process or cannot unduly influence the impartiality of the assessor or assessment team conducting the assessment of the security controls in the information system. [NIST SP 800-53]
Independent Verification and Validation (IV&V)	An independent assessment of a system. The assessment assures that the system conforms to the requirements and design, as documented, and fulfills the operational objectives.

Term	Definition
Individual	1. An assessment object that includes people applying specifications, mechanisms, or activities. [NIST SP 800-53A] 2. Person who is the subject of protected health information (PHI). [HIPAA]
Information	1. An instance of an information type. [NIST SP 800-39] 2. Any communication or reception of knowledge, such as facts, data, or opinions, including numerical, graphic, or narrative forms, whether oral or maintained in any other medium, including computerized databases, paper, microform, or magnetic tape. [OMB Circular A-130]
Information Assurance	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. [CNSSI-4009]
Information Owner	Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal. [NIST SP 800-53; CNSSI 4009]
Information Remnance	Control of information system remnance, sometimes referred to as object reuse, or data remnance, prevents information, including encrypted representations of information, produced by the actions of a prior user/role (or the actions of a process acting on behalf of a prior user/role) from being available to any current user/role (or current process) that obtains access to a shared system resource (e.g., registers, main memory, secondary storage) after that resource has been released back to the information system. [NIST SP 800-53]
Information Resource	Information and related resources, such as personnel, equipment, funds, and information technology. [44 USC Sec. 3502] Also see Resource.
Information Resource Owner	See Business Owner.
Information 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. [44 USC Sec. 3542]
Information Security Policy	Aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information. [CNSSI 4009]
Information Security Testing	The process of validating the effective implementation of security controls for information systems and networks, based on the organization's security requirements. [NIST SP 800-115]
Information Sharing	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. [44 USC Sec. 3502; OMB Circular A-130, App. III]

Term	Definition
Information System	1. A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. [44 USC Sec. 3502] 2. A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information in accordance with defined procedures, whether automated or manual. [OMB Circular A-130, Appendix III]
Information System Media	Includes both digital media (e.g., diskettes, magnetic tapes, external/ removable hard drives, flash/thumb drives, compact disks [CD], digital video disks [DVD]) and non-digital media (e.g., paper, microfilm). [NIST SP 800-53]
Information System Owner	See Business Owner.
Information System Security	The protection afforded to information systems to preserve the confidentiality, integrity, and availability, of the systems and information contained in the systems. (Protection results from the application of a combination of security measures, including crypto-security, transmission security, emission security, computer security, information security, personnel security, resource security, and physical security.) [NISTIR 4659] Also see System Security.
Information System Security Engineering	Process that captures and refines information security requirements and ensures their integration into information technology component products and information systems through purposeful security design or configuration. [NIST SP 800-37]
Information System Security Officer (ISSO)	1. Person responsible for ensuring the security of an information system throughout its life-cycle, from design through disposal. Synonymous with System Security Officer (SSO). [CNSSI 4009] 2. Individual assigned responsibility by the senior agency information security officer, authorizing official, management official, or information system owner for maintaining the appropriate operational security posture for an information system or program. [NIST SP 800-53]

Term	Definition
Information Technology (IT)	1. The term "information technology" — a. with respect to an executive agency means any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the 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 that requires the use - (1) of that equipment; or (2) of that equipment to a significant extent in the performance of a service or the furnishing of a product; b. includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources; but c. does not include any equipment acquired by a federal contractor incidental to a federal contract. [40 USC Sec. 11101] 2. 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 the executive agency. For purposes of the preceding sentence, 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. [NIST SP 800-53]
Information Type	A specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization or in some instances, by a specific law, Executive Order, directive, policy, or regulation. [FIPS 199]
Initial Program Load (IPL)	A program that brings another program, often the operating system, into operation to run the computer. Also referred to as a bootstrap or boot program. [FISCAM]
Input	Any information entered into a computer or the process of entering data into the computer. [FISCAM]
Inside Threat	An entity with authorized access that has the potential to harm an information system through destruction, disclosure, modification of data, and/or denial of service. [NIST SP 800-32]

Term	Definition
Integrity	1. The assurance that information and programs are changed only in a specified and authorized manner. 2. Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 USC Sec. 3542] 3. The property that sensitive data has not been modified or deleted in an unauthorized and undetected manner. [HIPAA] 4. With respect to data, its accuracy, quality, validity, and safety from unauthorized use. This involves ensuring that transmitted or stored data are not altered by unauthorized persons in a way that is not detectable by authorized users. [FISCAM]
Interconnection Security Agreement (ISA)	1. An agreement established between systems that share data and are owned or operated by different organizations. An ISA is required when the system interconnection/information sharing is between a CMS system and a system located external to the CMS secure network infrastructure. 2. An agreement established between the organizations that own and operate connected IT systems to document the technical requirements of the interconnection. The ISA also supports a Memorandum of Understanding or Agreement (MOU/A) between the organizations. [NIST SP 800-47]
Interface	A connection between two devices, applications, or networks or a boundary across which two systems communicate. Interface may also refer to the portion of a program that interacts with the user. [FISCAM]
Internal Connectivity	A computer or network connection to an organizational peer system within the defined security perimeter.
Internal Control	A process, implemented by agency management and other personnel, designed to provide reasonable assurance that (i) operations, including the use of agency resources, are effective and efficient; (ii) financial reporting, including reports on budget execution, financial statements, and other reports for internal and external use, are reliable; and (iii) applicable laws and regulations are followed. Internal control also includes the safeguarding of agency assets against unauthorized acquisition, use, or disposition. Internal control consists of five interrelated components that form an integrated process that can react to changing circumstances and conditions within the agency. These components include the control environment, risk assessment, control activities, information and communication, and monitoring. Also referred to as Internal Control Structure. [FISCAM]
Internal Security Testing	Security testing conducted from inside the organization's security perimeter. [NIST SP 800-115]
Internet	Refers to the collection of networks and gateways that use the Transmission Control Protocol/Internet Protocol (TCP/IP) suite of protocols. [FISCAM]
Interview	A type of assessment method that is characterized by the process of conducting discussions with individuals or groups within an organization to facilitate understanding, achieve clarification, or lead to the location of evidence, the results of which are used to support the determination of security control effectiveness over time. [NIST SP 800-53A]

Term	Definition
Intranet	A network internal to an organization but that runs the same protocols as the network external to the organization. Every organizational network that runs the Transmission Control Protocol/Internet Protocol (TCP/IP) suite is an intranet. [NIST SP 800-41]
Intrusion	Unauthorized access to logical and physical resources.
Intrusion Detection and Prevention System (IDPS)	Software that automates the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents and attempting to stop detected possible incidents. [NIST SP 800-61]
Intrusion Detection System (IDS)	Methods to track system activities to determine if current actions are consistent with the established policies and so that system administrators can identify inconsistencies that may signal unauthorized access.
Intrusion Prevention System	System that can detect an intrusive activity and can attempt to stop the activity, ideally before it reaches its targets. [NIST SP 800-36]
Investigation	The review and analysis of system security features (e.g., the investigation of system control programs using flow charts, assembly listings, and related documentation) to determine the security provided by the operating system.
IP Security (IPsec)	Request for Comments (RFC) 2411, protocol that provides security capabilities at the Internet Protocol (IP) layer of communications. IPsec's key management protocol is used to negotiate the secret keys that protect virtual private network (VPN) communications, and the level and type of security protections that will characterize the VPN. The most widely used key management protocol is the Internet Key Exchange (IKE) protocol. [NIST SP 800-46]
IT Project	A temporary planned endeavor funded by an approved information technology investment; thus achieving a specific goal and creating a unique product, service, or result. A project has a defined start and end point with specific objectives that, when attained signify completion. [DHHS Glossary of Key Enterprise Terms]

1.1.10 J

Term	Definition
Jamming	Transmission of electronic signals that disrupt communication and the use of electronic data.
Job	A set of data that completely defines a unit of work for a computer. A "job" usually includes programs, linkages, files, and instructions to the operating system. [FISCAM]

1.1.11 K

Term	Definition
Kerberos	A widely used authentication protocol developed at Massachusetts Institute of Technology (MIT). In "classic" Kerberos, users share a secret password with a Key Distribution Center (KDC). The user, Alice, who wishes to communicate with another user, Bob, authenticates to the KDC and is furnished a "ticket" by the KDC to use to authenticate with Bob. When Kerberos authentication is based on passwords, the protocol is known to be vulnerable to off-line dictionary attacks by eavesdroppers who capture the initial user-to-KDC exchange. [NIST SP 800-63]
Kernel Flaw	Any security flaw that occurs in the kernel code of an operating system.
Key	1. In cryptography, a key is a variable value that is applied using an algorithm to a string or block of unencrypted text to produce encrypted text, or to decrypt encrypted text. 2. A long stream of seemingly random bits used with cryptographic algorithms. The keys must be known or guessed to forge a digital signature or decrypt an encrypted message. [FISCAM]
Key Management	The activities involving the handling of cryptographic keys and other related security parameters (e.g., initialization vectors, passwords) during the entire life cycle of the keys, including their generation, storage, establishment, entry and output, and zeroization. [FIPS 140-2]
Keystroke Monitoring	1. A specialized form of audit trail software, or a specially designed device, that records every key struck by a user and every character of the response that the automated information system (AIS) returns to the user. 2. The process used to view or record both the keystrokes entered by a computer user and the computer's response during an interactive session. Keystroke monitoring is usually considered a special case of audit trails. [NIST SP 800-12]

1.1.12 L

Term	Definition
Label	The marking of an item or information to reflect its information category and/or security classification. Also see Security Label.
Least Privilege	1. The principle that requires each user be granted the most restrictive set of privileges needed for the performance of authorized tasks. The application of this principle limits the damage that can result from accident, error, or unauthorized use. 2. The security objective of granting users only those accesses they need to perform their official duties. [NIST SP 800-12]

Term	Definition
Library	1. A program library is a collection of (usually) pre-compiled, reusable programming routines that a programmer can "call" when writing code. 2. In computer terms, a "library" is a collection of similar files, such as data sets contained on tape and/or disks, stored together in a common area. Typical uses are to store a group of source programs or a group of load modules. In a "library", each program is called a member. "Libraries" are also called partitioned data sets (PDS). A "library" can also be used to refer to the physical site where magnetic media, such as a magnetic tape, is stored. These sites are usually referred to as tape "libraries". [FISCAM]
Library Control (or Management)	The function responsible for controlling program and data files that are either kept on-line or are on tapes and disks that are loaded onto the computer as needed. [FISCAM]
Library Management Software	Software that provides an automated means of inventorying software, ensuring that differing versions are not accidentally misidentified, and maintaining a record of software changes. [FISCAM]
Life-Cycle Process (or Life-Cycle Model)	1. Spans the entire time that a project/program including hardware and software is being planned, designed, developed, procured, installed, used, and retired from service. 2. A framework containing the processes, activities, and tasks involved in the development, operation, and maintenance of a software product, spanning the life of the system from the definition of its requirements to the termination of its use. [ISO/IEC 12207]
Likelihood of Occurrence	Estimation of the frequency or probability of a threat occurring based upon the ease of exploiting system vulnerabilities.
Limited Background Investigation (LBI)	This investigation consists of a National Agency Check and Inquiries (NACI), credit search, personal subject interview, and personal interviews by an investigator of subject's background during the most recent three years. [DHHS *Personnel Security/Suitability Handbook*]
Link Encryption	Link encryption encrypts all of the data along a communications path (e.g., a satellite link, telephone circuit, or T1 line). Since link encryption also encrypts routing data, communications nodes need to decrypt the data to continue routing. [NIST SP 800-12]
Load Library	A partitioned data set (PDS) used for storing load modules for later retrieval. [FISCAM]
Load Module	The results of the link edit process. An executable unit of code loaded into memory by the loader. [FISCAM]
Local Access	Access to an organizational information system by a user (or an information system) communicating through an internal organization-controlled network (e.g., local area network) or directly to a device without the use of a network. [NIST SP 800-53A]

Term	Definition
Local Area Network (LAN)	1. An interconnected computing environment that enables data sharing at a single location. This type of network does not utilize a public carrier. 2. A group of computers and other devices dispersed over a relatively limited area and connected by a communications link that enables a device to interact with any other on the network. 3. A group of computers and other devices dispersed over a relatively limited area and connected by a communications link that enables a device to interact with any other on the network. LANs commonly include microcomputers and shared resources such as laser printers and large hard disks. Most LANs can support a wide variety of computers and other devices. Separate LANs can be connected to form larger networks. [FISCAM]
Logging	The process of recording a pre-defined set of individual activities in electronic or paper format. The logging process can be automatic (computer system) or manual (logbook), and serves as the basis for establishing audit trails.
Logic Bomb	In programming, a form of sabotage in which a programmer inserts code that causes the program to perform a destructive action when some triggering event occurs, such as terminating the programmer's employment. [FISCAM]
Logical Access Control	1. A technical means of controlling what information users can utilize, the programs they can run, and the modifications they can make. 2. The use of computer hardware and software to prevent or detect unauthorized access. For example, users may be required to input user identification numbers (ID), passwords, or other identifiers that are linked to pre-determined access privileges. [FISCAM]
Log-off	The process of terminating a connection with a computer system or peripheral device in an orderly way. [FISCAM]
Log-on (Log-in)	The process of establishing a connection with, or gaining access to, a computer system or peripheral device. [FISCAM]
Logs or Logging File	1. A record of a computer's, network's, or application's activity, used for system information, backup, and recovery. 2. With respect to computer systems, a record of an event or transaction. [FISCAM] Also see Record.
Loss	The unrecoverable business resources that are redirected interrupted or removed from a system. Such losses may be loss of life, financial, public image, facilities, or operational capability.
Low Impact System	An information system in which all three security objectives (i.e., confidentiality, integrity, and availability) are assigned a FIPS 199 potential impact value of low. [FIPS 200]

1.1.13 M

Term	Definition
Macro Virus	A virus that attaches itself to documents and uses the macro programming capabilities of the document's application to execute and propagate. [NIST SP 800-61]
Mainframe System	A multi-user computer designed to meet the computing needs of a large organization. The term came to be used generally to refer to the large central computers developed in the late-1950s and 1960s to meet the accounting and information management needs of large organizations. [FISCAM]
Maintenance	1. Periodic upkeep of computer systems including clearing of log files, installation of patches and system upgrades. 2. Altering programs after they have been in use for a while. Maintenance programming may be performed to add features, correct errors that were not discovered during testing, or update key variables (such as the inflation rate) that change over time. [FISCAM] 3. The process of retaining a hardware system or component in, or restoring it to, a state in which it can perform its required functions. [IEEE Std 610.12-1990]
Major Application (MA)	1. A MA consists of data and application software only. It is housed on one or more General Support Systems (GSSs), supports the same major functions, and is under the same management control; either directly or indirectly. 2. An application that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, modification, or unauthorized access to the information in the application. Note: All federal applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight and should be treated as major. Adequate security for other applications should be provided by security of the systems in which they operate. [OMB Circular A-130, App. III]
Malicious Code	1. Unauthorized, subverting programs or code introduced into organizational software with the intent to, and purpose of, causing damage to data, applications, or networks. Malicious code includes viruses, time bombs, logic bombs, Trojan horses, and worms. 2. Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code. [NIST SP 800-61; CNSSI 4009]
Malware	A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim. [NIST SP 800-83]

Term	Definition
Management Control	The security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information system security. [FIPS 200]
Mandatory Access Control (MAC)	1. A means of restricting access to system resources based on the sensitivity (as represented by a label) of the information contained in the system resource and the formal authorization (i.e., clearance) of users to access information of such sensitivity. [NIST SP 800-44] 2. Access controls (which) are driven by the results of a comparison between the user's trust level or clearance and the sensitivity designation of the information. [FIPS 191]
Man-in-the-Middle (MitM) Attack	An attack on the authentication protocol, where the attacker positions themself between the claimant and verifier so that they can intercept and alter data traveling between them. [NIST SP 800-63]
Master Console	In multiple virtual storage (MVS) environments, the master console provides the principal means of communicating with the system. Other multiple console support consoles often serve specialized functions, but can have master authority to enter all MVS commands. [FISCAM]
Master File	1. A collection of records pertaining to information in a system such as customers, employees, products, and vendors. Master files contain information such as descriptive data, name and address, and summary information. 2. In a computer, the most currently accurate and authoritative permanent or semi-permanent computerized record of information maintained over an extended period. [FISCAM]
Material	Refers to data processed, stored, or used in and information generated by an automated data processing (ADP) system regardless of form or medium (e.g., programs, reports, data sets or files, records, and data elements).
Maximum Tolerable Downtime (MTD)	The amount of time mission/business process can be disrupted without causing significant harm to the organization's mission. [NIST SP 800-34]
Mechanism	An assessment object that includes specific protection-related items (e.g., hardware, software, or firmware) employed within or at the boundary of an information system. [NIST SP 800-53A]
Media (Storage)	1. Physical objects such as paper, personal computers, and workstation diskettes, compact disc-read-only memory (CD-ROMs), and other forms by which CMS data is stored or transported. The risk to exposure is considered greater when data is in an electronically readable and transmittable form than when the same data is in paper-only form. This is due to the greater volume of information that can be sent in electronic form, the ease and convenience with which the information can be transmitted, and the potential for such information to be intercepted or sent inadvertently to the wrong person or entity. 2. Includes both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks [CD], digital video disks [DVD]) and non-digital media (e.g., paper, microfilm). [NIST SP 800-53]

Term	Definition
Media Sanitization	1. A general term referring to the actions taken to render data written on media unrecoverable by both ordinary and extraordinary means. [NIST SP 800-88] 2. The process used to remove information from information system media such that there is a reasonable assurance, in proportion to the confidentiality of the information, that the information cannot be retrieved or reconstructed. [NIST SP 800-53]
Medium	Material on which data are or may be recorded, such as paper, punched cards, magnetic tape, magnetic disks, solid state devices, or optical discs. [NIST SP 800-88]
Memorandum of Understanding/Agreement (MOU/MOA)	1. An instrument used when agencies enter into a joint project in which they each contribute their own resources in which the scope of work is very broad and not specific to any one project; or in which there is no exchange of goods or services between the participating agencies. 2. An agreement established between systems that share data and are owned or operated by different organizations. An MOU is required when the system interconnection/information sharing is between two or more CMS systems located internal to the CMS secure network infrastructure.
Message Authentication Code (MAC)	A cryptographic checksum on data that uses a symmetric key to detect both accidental and intentional modifications of the data. [FIPS 201; NIST SP 800-63]
Metrics	Tools designed to facilitate decision-making and improve performance and accountability through collection, analysis, and reporting of relevant performance-related data. [NIST SP 800-55]
Migration	A change from an older hardware platform, operating system, or software version to a newer one. [FISCAM]
Min-Entropy	A measure of the difficulty that an attacker has to guess the most commonly chosen password used in a system. When a password has n-bits of min-entropy then an attacker requires as many trials to find a user with that password as is needed to guess an n-bit random quantity. The attacker is assumed to know the most commonly used password(s).
Minimum Background Investigation (MBI)	This investigation includes a National Agency Check and Inquiries (NACI), a credit record search, a face-to-face personal interview between the investigator and the subject, and telephone inquiries to selected employers. The MBI is an enhanced version of the National Agency Check and Inquiries and Credit Check (NACIC) and can be used for selected public trust positions. [DHHS *Personnel Security/Suitability Handbook*]
Mission Critical	1. The systems that support a core business process are called mission- critical systems. The absence or failure of mission-critical systems could have a significant impact on the mission, operations and viability of the organization. 2. Any telecommunications or information system that is defined as a national security system (i.e., FISMA) or processes any information the loss, misuse, disclosure, or unauthorized access to or modification of, would have a debilitating impact on the mission of an agency. [NIST SP 800-60R1, Vol. 2]

Term	Definition
Misuse of Government Property	The use of computer systems for other than official business that does not involve a criminal violation but is not permissible under CMS policies.
Mobile Code	Software programs or parts of programs obtained from remote information systems, transmitted across a network, and executed on a local information system without explicit installation or execution by the recipient. [NIST SP 800-53A]
Mobile Code Technologies	Software technologies that provide the mechanisms for the production and use of mobile code (e.g., Java, JavaScript, ActiveX, VBScript, portable document format [PDF], Shockwave movies, Flash animations). [NIST SP 800-53A]
Modem	Short for modulator-demodulator. A device that allows digital signals to be transmitted and received over analog telephone lines. This type of device makes it possible to link a digital computer to the analog telephone system. It also determines the speed at which information can be transmitted and received. [FISCAM]
Moderate Impact System	An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of moderate and no security objective is assigned a FIPS 199 potential impact value of high. [FIPS 200]
Modification	Loss of integrity of an asset or asset group through the intentional or unintentional alteration of the asset or asset group.
Monitoring	The process of observing, supervising, or controlling system, network, or physical activities on a real-time and continuous basis.

1.1.14 N

Term	Definition
National Agency Check (NAC)	An integral part of all background investigations, the NAC consists of searches of OPM's Security/Suitability Investigations Index (SII); the Defense Clearance and Investigations Index (DCII); the Federal Bureau of Investigation (FBI) Identification Division's name and fingerprint files, and other files or indices when necessary. [DHHS *Personnel Security/Suitability Handbook*]
National Agency Check and Inquiries (NACI)	This is the basic and minimum investigation required on all new federal employees. It consists of a National Agency Check (NAC) with written inquiries and searches of records covering specific areas of a person's background during the past five years. Those inquiries are sent to current and past employers, schools attended, references, and local law enforcement authorities. [DHHS *Personnel Security/Suitability Handbook*]
National Agency Check and Inquiries and Credit Check (NACIC)	This National Agency Check and Inquiries (NACI) includes the addition of a credit record search and is the minimum investigation for those going into low risk public trust positions (Level 5). [DHHS *Personnel Security/Suitability Handbook*]
National Security Position	Sensitive position (designated as Level 2, 3, or 4) in which the incumbents' duties and/or responsibilities involve access to classified information or other restricted information relating to the security of our nation. [DHHS *Personnel Security/Suitability Handbook*]

Term	Definition
Need-to-Know	The necessity for access to, or knowledge or possession of, specific information required to carry out official duties. [CNSSI 4009]
Network	1. A telecommunications medium that, with associated components, is a means of exchanging information. 2. An open communications medium, typically the Internet, which is used to transport messages between the claimant and other parties. Unless otherwise stated, no assumptions are made about the security of the network; it is assumed to be open and subject to active (e.g., impersonation, man-in-the-middle, session hijacking…) and passive (e.g., eavesdropping) attack at any point between the parties (i.e., claimant, verifier, CSP or relying party). 3. A group of computers and associated devices that are connected by communications facilities. A network can involve permanent connections, such as cables, or temporary connections made through telephone or other communications links. A network can be as small as a local area network consisting of a few computers, printers, and other devices, or it can consist of many small and large computers distributed over a vast geographic area. [FISCAM]
Network Architecture	The description of an information-sharing environment.
Network Discovery	The process of discovering active and responding hosts on a network, identifying weaknesses, and learning how the network operates. [NIST SP 800-115]
Network Interface	The point of interconnection for a single node to a network environment.
Network Mapping	The process of identifying a network structure or architecture, including the placement and configuration of network components (servers, routers, firewalls, etc.).
Network Protocols	The rules and conventions for communication between devices. Protocol definitions include formatting rules that specify how data is packaged into messages, message acknowledgement conventions, and data compression conventions.
Network Sniffing	A passive technique that monitors network communication, decodes protocols, and examines headers and payloads for information of interest. It is both a review technique and a target identification and analysis technique. [NIST SP 800-115]
Network-based Intrusion Detection System	Intrusion Detection Systems (IDSs) which detect attacks by capturing and analyzing network packets. [NIST SP 800-36]
Nonce	A value used in security protocols that is never repeated with the same key. For example, challenges used in challenge-response authentication protocols generally must not be repeated until authentication keys are changed, or there is a possibility of a replay attack. Using a nonce as a challenge is a different requirement from a random challenge, because a nonce is not necessarily unpredictable. [NIST SP 800-63]
Non-privileged Access	Cannot bypass any security controls.

Term	Definition
Non-repudiation	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. [NIST SP 800-39]
Non-sensitive Position	Positions (designated as Level 1) which are neither Public Trust nor National Security positions. [DHHS *Personnel Security/Suitability Handbook*]

1.1.15 O

Term	Definition
Object	A passive entity that contains or receives information. [NIST SP 800-27A]
Object Code	The machine code generated by a source code language processor such as an assembler or compiler. A file of object code may be executable immediately or it may require linking with other object code files (e.g., libraries, to produce a complete executable program). [FISCAM]
Office of Information Services (OIS)	CMS office that ensures the effective management of CMS' information systems and resources. The office also develops and maintains central databases and statistical files, and directs Medicare claims payment systems.
Off-line	1. Off-line units are not available for immediate use on demand by the system. [FS 1037C] 2. Pertaining to equipment that is disconnected from a system, is not in operation, and usually has its main power source disconnected or turned off. [FS 1037C]
Off-line Attack	An attack where the attacker obtains some data (typically by eavesdropping on an authentication protocol run, or by penetrating a system and stealing security files) that s/he is able to analyze in a system of his/her own choosing.
Off-site Storage Facility	A secure location, remote from the primary location, at which backup hardware, software, data files, documents, equipment, or supplies are stored for backup or other purposes.
On-line	1. On-line units are available for immediate use on demand by the system without human intervention. [FS 1037C] 2. Pertaining to equipment that is connected to a system, and is in operation. [FS 1037C]
On-line Attack	An attack against an authentication protocol where the attacker either assumes the role of a claimant with a genuine verifier or actively alters the authentication channel. The goal of the attack may be to gain authenticated access or learn authentication secrets.
On-line Certificate Status Protocol (OCSP)	An on-line protocol used to determine the status of a public key certificate. See [RFC 2560].
On-line System	See On-line.

Term	Definition
Operating System (OS)	1. An operating system (sometimes abbreviated as “OS”) is the program that, after being initially loaded into the computer by a boot program, manages all the other programs in a computer. The purpose of an OS is to provide an environment in which a user can execute programs in a convenient and efficient manner. 2. The software “master control application” that runs the computer. It is the first program loaded when the computer is turned on, and its principal component, the kernel, resides in memory at all times. The OS sets the standards for all application programs (such as the mail server) that run in the computer. The applications communicate with the OS for most user interface and file management operations. [NIST SP 800-45]
Operational Control	1. The day-to-day security procedures and mechanisms to protect operational systems. The operational controls consist of the physical, environmental and personnel security controls. 2. The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by people (as opposed to systems). [FIPS 200]
Organization	A federal agency or, as appropriate, any of its operational elements. [FIPS 200]
Output	Data/information produced by computer processing, such as graphic display on a terminal or hard copy. [FISCAM]
Output Device	Peripheral equipment, such as a printer or tape drive, that provides the results of processing in a form that can be used outside the system. [FISCAM]
Outside Threat	An unauthorized entity from outside the domain perimeter that has the potential to harm an Information System through destruction, disclosure, modification of data, and/or denial of service. [NIST SP 800-32]
Overt Testing	Security testing performed with the knowledge and consent of the organization’s information technology staff. [NIST SP 800-115]
Overwrite	Writing patterns of data on top of the data stored on a magnetic medium. The National Security Agency (NSA) has researched that one overwrite is good enough to sanitize most drives. [NIST SP 800-88]
Owner	See Business Owner.

1.1.16 P

Term	Definition
Packet Filtering	A process to ensure data is allowed to enter or leave the computing environment only if firewall rules allow it. As packets arrive they are filtered according to their type, source address, destination address, and port information contained in each packet.
Packet Sniffer	Software that observes and records network traffic. [NIST SP 800-61]
Parameter	A value that is given to a variable. Parameters provide a means of customizing programs. [FISCAM]
Partitioning	The act of logically dividing a media into portions that function as separate units. [NIST SP 800-111]

Term	Definition
Passive Attack	An attack against an authentication protocol where the attacker intercepts data traveling along the network between the claimant and verifier, but does not alter the data (i.e., eavesdropping). [NIST SP 800-63]
Password	1. Most often associated with user authentication. However, they are also used to protect data and applications on many systems, including personal computers (PCs). Password-based access controls for PC applications are often easy to circumvent if the user has access to the operating system (and knowledge of what to do). 2. A protected string and/or character of symbols that is used to permit computer access by authenticating a particular user. A secret combination of alphanumeric characters that a claimant memorizes and uses to authenticate his or her identity. Passwords are typically character strings. 3. A string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization. [FIPS 140-3]
Password Cracking	The process of recovering secret passwords stored in a computer system or transmitted over a network. [NIST SP 800-115]
Patch	An additional piece of code developed to address a problem in an existing piece of software. [NIST SP 800-40]
Patch Management	The process of acquiring, testing, and distributing patches to the appropriate administrators and users throughout the organization. [NIST SP 800-61]
Penetration	1. The successful act of bypassing the security mechanisms of a system or application. 2. Unauthorized act of bypassing the security mechanisms of a system. [CNSSI 4009]
Penetration Testing	1. Security testing in which evaluators mimic real-world attacks in an attempt to identify ways to circumvent the security features of an application, system, or network. Penetration testing often involves issuing real attacks on real systems and data, using the same tools and techniques used by actual attackers. Most penetration tests involve looking for combinations of vulnerabilities on a single system or multiple systems that can be used to gain more access than could be achieved through a single vulnerability. [NIST SP 800-115] 2. A test methodology in which assessors, using all available documentation (e.g., system design, source code, manuals) and working under specific constraints, attempt to circumvent the security features of an information system. [NIST SP 800-53A]
Peripheral	A hardware unit that is connected to and controlled by a computer, but external to the central processing unit (CPU). These devices provide input, output, or storage capabilities when used in conjunction with a computer. [FISCAM]

Term	Definition
Personal Data	Data about an individual including, but not limited to, education, financial transactions, medical history, qualifications, service data, criminal or employment history which ties the data to the individual's name, or an identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice-print or a photograph.
Personal Digital Assistant (PDA)	A handheld computer that serves as a tool for reading and conveying documents, electronic mail, and other electronic media over a communications link, and for organizing personal information, such as a name-and-address database, a to-do list, and an appointment calendar. [NIST SP 800-124]
Personal Health Information	See Protected Health Information (PHI).
Personal Identification Number (PIN)	1. An individual's access code commonly used to authenticate the bearer of a magnetic card or other physical identification device; logically equivalent to either user identification code or a password. 2. A secret that a claimant memorizes and uses to authenticate his or her identity. PINs are generally only decimal digits. [FIPS 201]
Personal Identity Verification (PIV) Card	Physical artifact (e.g., identity card, "smart" card) issued to an individual that contains stored identity credentials (e.g., photograph, cryptographic keys, digitized fingerprint representation etc.) such that a claimed identity of the cardholder may be verified against the stored credentials by another person (human readable and verifiable) or an automated process (computer readable and verifiable). [FIPS 201]
Personally Identifiable Information (PII)	1. Any information about an individual including, but not limited to, education, financial transactions, medical history, and criminal or employment history, and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information, which is linked or linkable to an individual. 2. Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. [OMB M-07-16]
Personnel Control	This type of control involves screening individuals prior to their authorization to access computer resources. Such screening should be commensurate with the risk and magnitude of the harm the individual could cause. [FISCAM]

Term	Definition
Personnel Security	1. Procedures that are established to ensure that all personnel who have access to sensitive information have the required authority as well as appropriate clearances. Procedures to ensure a person's background is as presented; provide assurance of necessary trustworthiness. 2. Refers to the procedures established to ensure that each individual has a background that indicates a level of assurance of trustworthiness, which is commensurate with the value of automated data processing (ADP) resources, which the individual will be able to access. [NISTIR 4659] Also see Personnel Control.
Phishing	1. A digital form of social engineering that uses authentic-looking—but bogus—emails to request information from users or direct them to a fake Web site that requests information. [NIST SP 800-115] 2. Tricking individuals into disclosing sensitive personal information through deceptive computer-based means. [NIST SP 800-83]
Physical Access Control	This type of control involves restricting physical access to computer resources and protecting these resources from intentional or unintentional loss or impairment. [FISCAM]
Physical and Environmental Control	Protective mechanisms in the area where application processing takes place, or for the General Support System (GSS) (e.g., locks on terminals, physical barriers around the building and processing area, air-conditioning, etc.). Factors to address include physical access, fire safety, failure of supporting utilities, structural collapse, plumbing leaks, interception of data, and mobile and portable systems.
Physical Destruction	A sanitization method for optical media, such as compact discs (CD). [NIST SP 800-88]
Physical Intrusion	Unauthorized access to or use of physical resources, including but not limited to facilities, wiring closets, and power supplies.
Physical Safeguard	Physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment from natural and environmental hazards, and unauthorized intrusion. [HIPAA]
Physical Security	Refers to the application of physical barriers and control procedures as preventive measures and countermeasures against threats to resources and sensitive information. [NISTIR 4659] Also see Physical Access Control; and Physical and Environmental Control.
Plaintext	Intelligible data that has meaning and can be understood without the application of decryption. [NIST SP 800-21]
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. The purpose of this 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. [OMB M-02-01]

Term	Definition
Policy	An official statement of a position, plan or course of action established by an identified sponsoring authority, which is designed to influence, to provide direction and to determine decisions and actions with regard to a specific topic. Policies provide broad direction or goals. Standards, procedures, and guidelines flow from policies. Also see Security Policy.
Policy Guideline	An example of how a policy might be applied to a specific situation. An outline or checklist of detailed procedures recommended satisfying a policy.
Port	An interface between the central processing unit (CPU) of the computer and a peripheral device that governs and synchronizes the flow of data between the CPU and the external device. [FISCAM]
Port Scanner	A program that can remotely determine which ports on a system are open (e.g., whether systems allow connections through those ports). [NIST SP 800-115]
Portable and Mobile Devices	Includes notebook computers, personal digital assistants, cellular telephones; and other computing and communications devices with network connectivity and the capability of periodically operating in different physical locations. [NIST SP 800-53]
Position Sensitivity	The degree of risk and level of relative importance assigned to a specific position. [DHHS *Personnel Security/Suitability Handbook*]
Possession and Control of a Token	The ability to activate and use the token in an authentication protocol.
Potential Impact	The loss of confidentiality, integrity, or availability could be expected to have: • A limited adverse effect [FIPS 199 Low]; • A serious adverse effect [FIPS 199 Moderate]; or • A severe or catastrophic adverse effect [FIPS 199 High] on organizational operations, organizational assets, or individuals. [NIST SP 800-39; Adapted from FIPS 199]
Practice Statement	A formal statement of the practices followed by an authentication entity (e.g., Registration Authority, Credentials Service Provider, or Verifier); typically, the specific steps taken to register and verify identities, issue credentials and authenticate claimants.
Privacy	1. The right of individuals to control or influence information that is related to them in terms of who may collect or store it and to whom that information may be disclosed. 2. The individual's right to privacy must be protected in federal government information activities involving personal information. Such information is to be collected, maintained, and protected to preclude intrusion into the privacy of individuals and the unwarranted disclosure of personal information. [OMB Circular A-130]
Privacy Act	The privacy to which individuals are entitled under 5 USC Sec. 552a, but that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

Term	Definition
Privacy Act Data	Personal data, which includes information pertaining to an individual's health or physical condition, job performance, investigatory or personal information about individuals that could cause embarrassment or damage to their reputations.
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. [OMB M-03-22]
Privacy Information	The individual's right to privacy must be protected in federal government information activities involving personal information. Such information is to be collected, maintained, and protected to preclude intrusion into the privacy of individuals and the unwarranted disclosure of personal information. [OMB Circular A-130]
Private Key	The secret part of an asymmetric key pair that typically is used to sign or decrypt data digitally.
Privilege	1. The rights to alter, circumvent, override, or bypass the operating system or system security measures. 2. Set of access rights permitted by the access control system. [FISCAM]
Privileged Access	Can bypass, modify, or disable the technical or operational system security controls.
Privileged Account	Individuals who have access to set "access rights" for users on a given system. Sometimes referred to as system or network administrative accounts. [NIST SP 800-12]
Privileged Function	A function executed on an information system involving the control, monitoring, or administration of the system. [NIST SP 800-53]
Privileged User	Individual who has access to system control, monitoring, or administration functions (e.g., system administrator, information system security officer, maintainer, system programmer). [CNSSI 4009]
Probe	Attempt to gather information about an information system or its users. [CNSSI 4009]
Procedure	1. A series of steps followed in a regular definite order. 2. A course of action to be taken to perform a given task.
Processing	The execution of program instructions by the computer's central processing unit. [FISCAM]
Product	A physical entity (e.g., a piece of hardware or software) or artifact (e.g., a document) that is created by someone or some process.
Production Environment	The system environment where the agency performs its operational information processing activities. [FISCAM]

Term	Definition
Production Input/Output Control	1. Methods used for the marking, handling, processing, storage, and disposal of input and output information and media, as well as labeling and distribution procedures for the information and media. 2. [Production control and scheduling] The function responsible for monitoring the information into, through, and as it leaves the computer operations area and for determining the succession of programs to be run on the computer. Often, an automated scheduling package is utilized in this task. [FISCAM]
Production Program	Programs that are being used and executed to support authorized organizational operations. Such programs are distinguished from "test" programs that are being developed or modified, but have not yet been authorized for use by management. [FISCAM]
Profile	A set of rules that describes the nature and extent of access to available resources for a user or a group of users with similar duties, such as accounts payable clerks. [FISCAM] Also see Standard Profile and User Profile.
Profiling	Measuring the characteristics of expected activity so that changes to it can be more easily identified. [NIST SP 800-61]
Program	1. A set of related instructions that, when followed and executed by a computer, perform operations or tasks. Application programs, user programs, system program, source programs, and object programs are all software programs. [FISCAM] 2. Consists of organized activity that contains a number of basic elements such as conducting risk assessments; conducting information technology security training; establishing an incident response capability; writing, establishing, and enforcing policies and procedures, and processes for planning, implementing, evaluating, and implementing remedial action for addressing weaknesses. [Title III of the E-Government Act]
Program Library	See Library.
Programmer	A person, who designs, codes, tests, debugs, and documents computer programs. [FISCAM]
Programming Library Software	A system that allows control and maintenance of programs for tracking purposes. The systems usually provide security, check out controls for programs, and on-line directories for information on the programs. [FISCAM]
Project Officer (PO)	CMS official (generally located in Central Office department) responsible for the oversight of other business partners. These include Common Working File (CWF) Host Sites, Durable Medical Equipment Regional Carriers (DMERCs), standard claims processing system maintainers, Regional Laboratory Carriers, and claims processing data centers.
Proof of Possession Protocol	A protocol where a claimant proves to a verifier that s/he possesses and controls a token (e.g., a key or password).
Proprietary	Privately owned, based on trade secrets, privately developed technology, or specifications that the owner refuses to divulge, thus preventing others from duplicating a product or program unless an explicit license is purchased. [FISCAM]

Term	Definition
Protected Health Information (PHI)	Individually identifiable health information that is: • Transmitted by electronic media, • Maintained in electronic media, or • Transmitted or maintained in any other form or medium. [HIPAA] Note: PHI excludes individually identifiable health information in employment records held by a covered HIPAA entity in its role as employer.
Protocol	In data communications and networking, a standard that specifies the format of data as well as the rules to be followed when performing specific functions, such as establishing a connection and exchanging data. [FISCAM]
Protocol Run	An instance of the exchange of messages between a claimant and a verifier in a defined authentication protocol that results in the authentication (or authentication failure) of the claimant.
Proxy	A proxy is an application that "breaks" the connection between client and server. The proxy accepts certain types of traffic entering or leaving a network, processes it, and forwards it. This effectively closes the straight path between the internal and external networks. Making it more difficult for an attacker to obtain internal addresses and other details of the organization's internal network. Proxy servers are available for common Internet services; for example, a hypertext transfer protocol (HTTP) proxy used for Web access, and an simple mail transfer protocol (SMTP) proxy used for e-mail. [NIST SP 800-44]
Proxy Server	A server that sits between a client application, such as a web browser, and a real server. It intercepts all requests to the real server to see if it can fulfill the requests itself. If not, it forwards the request to the real server. [NIST SP 800-46]
Pseudonym	A subscriber name that has been chosen by the subscriber that is not verified as meaningful by identity proofing. [NIST SP 800-63]
Public Access Control	A subset of access controls that apply when an agency application promotes or permits public access. These controls protect the integrity of the application and public confidence in the application and include segregating the information made directly available to the public from official agency records. [FISCAM]
Public Domain Software	1. Software, which has no copyright protection and can, be used or copied by anyone free of charge. 2. Software that has been distributed with an explicit notification from the program's author that the work has been released for unconditional use, including for-profit distribution or modification by any party under any circumstances. [FISCAM]
Public Information	1. Data available to the general population. The disclosures of this information are not expected to affect the agency seriously or adversely. Examples include general organizational information on the organization's web site, public brochures, and pamphlets. 2. Any information, regardless of form or format that an agency discloses, disseminates, or makes available to the public. [NIST SP 800-60 Vol. 2]

Term	Definition
Public Key	The public part of an asymmetric key pair that typically is used to verify signatures or encrypt data. [NIST SP 800-63]
Public Key Certificate	1. A digital document issued and digitally signed by the private key of a Certification Authority that binds the name of a subscriber to a public key. The certificate indicates that the subscriber identified in the certificate has sole control and access to the private key. [NIST SP 800-63] 2. A set of data that contains a unique identifier associated with an entity, contains the public key associated with the identifier, and is digitally signed by a trusted party, thereby binding the public key to the identifier. [FIPS 140-3]
Public Key Infrastructure (PKI)	1. Framework established to issue, maintain, and revoke Public Key certificates accommodating a variety of security Technologies, including the use of software. [CNSSI 4009] 2. An architecture which is used to bind public keys to entities, enable other entities to verify public key bindings, revoke such bindings, and provide other services critical to managing public keys. [FIPS 196]
Public Trust Position	Positions that have the potential for action or inaction by their incumbents to affect the integrity, efficiency, or effectiveness of assigned Government activities. The potential for adverse effects includes action or inaction that could diminish public confidence in the integrity, efficiency, or effectiveness of assigned Government activities, whether or not actual damage occurs. [5 CFR Part 731]
Pulverization	A physically destructive method of sanitizing media; the act of grinding to a powder or dust. [NIST SP 800-88]
Purge	Rendering sanitized data unrecoverable by laboratory attack methods. [NIST SP 800-88]

1.1.17 Q

Term	Definition
Quality Assurance	The function that reviews software project activities and tests software products throughout the software life-cycle to determine if: • The software project is adhering to its established plans, standards, and procedures, and • The software meets the functional specifications defined by the user. [FISCAM]

1.1.18 R

Term	Definition
Race Condition	The act of gaining higher-level privileges to a program or process before it has given up its privileged mode. Common race conditions include signal handling and core-file manipulation.
Read Access	This level of access provides the ability to look at and copy data or a software program. [FISCAM]

Term	Definition
Real-Time System	A computer and/or a software system that reacts to events before they become obsolete. This type of system is generally interactive and updates files as transactions are processed. [FISCAM]
Recertification	See Certification.
Record	1. Any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph. [Privacy Act of 1974] 2. The recordings (automated and/or manual) of evidence of activities performed or results achieved (e.g., forms, reports, test results), which serve as a basis for verifying that the organization and the information system are performing as intended. Also used to refer to units of related data fields (i.e., groups of data fields that can be accessed by a program and that contain the complete set of information on particular items). [FIPS 200] 3. A unit of related data fields. The group of data fields that can be accessed by a program and contains the complete set of information on a particular item. [FISCAM]
Recovery Point Objective (RPO)	The point in time to which data must be recovered after an outage. [NIST SP 800-34]
Recovery Procedure	Actions necessary to restore data files of an information system and computational capability after a system failure. [CNSSI 4009]
Recovery Time Objective (RTO)	The overall length of time an information system's components can be in the recovery phase before negatively affecting the organization's mission or mission/business processes. [NIST SP 800-34]
Registration	The process through which a party applies to become a subscriber of a Credentials Service Provider (CSP) and a Registration Authority validates the identity of that party on behalf of the CSP.
Registration Authority	A trusted entity that establishes and vouches for the identity of a subscriber to a Credentials Service Provider (CSP). The Registration Authority may be an integral part of a CSP, or it may be independent of a CSP, but it has a relationship to the CSP(s).
Reliability	The capability of hardware or software to perform consistently as the user expects, without failures or erratic behavior. [FISCAM]
Relying Party	An entity that relies upon the subscriber's credentials, typically to process a transaction or grant access to information or a system.
Remanence	Residual information remaining on storage media after clearing. [NIST SP 800-88]
Remediation	The act of correcting a vulnerability or eliminating a threat. Three possible types of remediation are installing a patch, adjusting configuration settings, and uninstalling a software application. [NIST SP 800-40]

Term	Definition
Remote Access	1. Access to an organizational information system by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet). Examples of remote access methods include dial-up, broadband, and wireless. [NIST SP 800-53] 2. The process of communicating with a computer located outside a network over a communications link. [FISCAM]
Remote Log-on	The act of gaining access to a machine across a network from a distant location through normal authentication methods. Generally, this implies a computer, a modem, and some remote access software to connect to the network.
Remote Maintenance	Maintenance and diagnostic activities conducted by individuals communicating through an external, non-organization-controlled network (e.g., the Internet). [NIST SP 800-53]
Remote Session	A session initiated whenever an organizational information system is accessed by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet). [NIST SP 800-53]
Research and Acknowledgement	The process of acknowledging a vulnerability and researching controls to remedy the weakness.
Residual Data	Data from deleted files or earlier versions of existing files. [NIST SP 800-111]
Residual Risk	1. A qualitative or quantitative substantiation of potential loss that remains after a mitigating control(s) has been implemented and is operational. 2. The potential risk remaining after all information technology security measures are applied. There is a residual risk associated with each threat. [NIST SP 800-33]
Residue	Data left in storage after information-processing operations are complete, but before degaussing or overwriting has taken place. [NIST SP 800-88]
Resource	1. Any function, device, or collection of data in an organization that can be allocated for use by users or programs. 2. Any agency automated information system (AIS) asset. [DHHS Definition] 3. Something that is needed to support computer operations, including hardware, software, data, telecommunications services, computer supplies such as paper stock and pre-printed forms, and other resources such as people, office facilities, and non-computerized records. [FISCAM]
Resource Access Control Facility (RACF)	An access control software package developed by IBM. [FISCAM]
Resource Owner	See Business Owner.
Restoration	The process of planning for and implementing business recovery, which enables the organization to return to a normal service level.

Term	Definition
Review and Approval	The process whereby information pertaining to the security and integrity of an automated data processing (ADP) activity or network is collected, analyzed, and submitted to the appropriate Designated Approving Authority (DAA) for accreditation of the activity or network.
Review Technique	Passive information security testing techniques, generally conducted manually, that are used to evaluate systems, applications, networks, policies, and procedures to discover vulnerabilities. They include documentation, log, rule-set, and system configuration review; network sniffing; and file integrity checking. [NIST SP 800-155]
Risk	1. A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. [NIST SP 800-39]
Risk Acceptance	Formal process by which an authorized management official agrees that no additional safeguards beyond those minimum controls required by, or already added to, the current *CMS Minimum Security Requirements* will be undertaken to control a specific documented risk.
Risk Analysis	1. A risk analysis involves identifying the most probable threats to a system and analyzing the related vulnerabilities of the system to these threats. 2. The identification and study of the vulnerability of a system and the possible threats to its security. [FIPS 11-3] 3. The process of identifying the risks to system security and determining the likelihood of occurrence, the resulting impact, and the additional safeguards that mitigate this impact. Part of risk management and synonymous with risk assessment. [NIST SP 800-27A]
Risk Assessment (RA)	1. The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. [NIST SP 800-39]
Risk Assumption	The acceptance of a potential risk and implementation of recommended controls or the continuation of operation without additional controls.
Risk Avoidance	The process of eliminating a risk by removing the cause (e.g., shut down the system at risk).
Risk Evaluation	This task includes the evaluation of all collected information regarding threats, vulnerabilities, assets, and asset values in order to measure the associated chance of loss and the expected magnitude of loss for each of an array of threats that could occur. Results are usually expressed in monetary terms on an annualized basis Annual Loss Expectancy (ALE) or graphically as a probabilistic “risk curve” for a quantitative risk assessment. For a qualitative risk assessment, results are usually expressed through a matrix of qualitative metrics such as ordinal ranking (low, medium, high, or 1, 2, 3).

Term	Definition
Risk Executive (function)	An individual or group within an organization that helps to ensure that: (i) security risk-related considerations for individual information systems, to include the authorization decisions for those systems, are viewed from an organization-wide perspective with regard to the overall strategic goals and objectives of the organization in carrying out its missions and business functions; and (ii) managing risk from individual information systems is consistent across the organization, reflects organizational risk tolerance, and is considered along with other organizational risks affecting mission/business success. [NIST SP 800-39]
Risk Levels	The extent to which a vulnerability could be exploited or the amount of damage that could be done. Risk levels are usually measured in a qualitative manner as high, moderate, or low.
Risk Limitation	The process of limiting a risk by implementing controls that contain and minimize the damage caused by the exploitation of a weakness.
Risk Management	1. The program and supporting processes to manage information security risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, and includes: (i) establishing the context for risk-related activities; (ii) assessing risk; (iii) responding to risk once determined; and (iv) monitoring risk over time. [NIST SP 800-39]
Risk Mitigation	Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process. [NIST SP 800-39]
Risk Monitoring	Maintaining ongoing awareness of an organization's risk environment, risk management program, and associated activities to support risk decisions. [NIST SP 800-39]
Risk Planning	The process of managing a risk by initiating a risk mitigation plan that ranks, implements and maintains controls.
Risk Response	Accepting, avoiding, mitigating, sharing, or transferring risk to organizational operations (i.e., mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation. [NIST SP 800-39]
Risk Response Measure	A specific action taken to respond to an identified risk. [NIST SP 800-39]
Risk Tolerance	The level of risk an entity is willing to assume in order to achieve a potential desired result. [NIST SP 800-32]
Risk Transference	The process of transferring a risk or the direct responsibility for bearing the risk from one party to a third party (e.g., flood insurance).
Roadmap	A central repository intended to provide summary, as well as detailed, information regarding approved CMS Policies, Processes, Procedures, Templates, Resources and Standards established for the successful engineering, implementation, maintenance and management of all CMS Information Technology (IT) projects. As such, the Roadmap provides Active Contributors on IT projects with an entry point to a wealth of information for successfully accomplishing the IT Investment Management Process and System Development Life Cycle (SDLC) at CMS

Term	Definition
Rogue Device	An unauthorized node on a network. [NIST SP 800-115]
Rootkit	A set of tools used by an attacker after gaining root-level access to a host to conceal the attacker's activities on the host and permit the attacker to maintain root-level access to the host through covert means. [NIST SP 800-61]
Router	1. Computer equipment connected to at least two separate networks that are responsible for forwarding network packets to the next point toward a specified destination. Routers can be hardware devices or software implemented within computer systems. 2. An intermediary device on a communications network that expedites message delivery. As part of a local area network (LAN), a router receives transmitted messages and forwards them to their destination over the most efficient available route. [FISCAM]
Rules of Behavior (ROB)	1. Guidelines describing permitted actions by users and their responsibilities when utilizing a computer system. 2. The rules that have been established and implemented concerning use of, security in and acceptable level of risk for the system. Rules will clearly delineate responsibilities and expected behavior of all individuals with access to the system. Rules should cover such matters as work at home, dial-in access, connection to the Internet, use of copyrighted works, unofficial use of federal government equipment, the assignment and limitation of system privileges, and individual accountability. [NIST SP 800-18]
Rules of Engagement (ROE)	Detailed guidelines and constraints regarding the execution of information security testing. The ROE is established before the start of a security test, and gives the test team authority to conduct defined activities without the need for additional permissions. [NIST SP 800-115]
Ruleset	A collection of rules or signatures that network traffic or system activity is compared against to determine an action to take—such as forwarding or rejecting a packet, creating an alert, or allowing a system event. [NIST SP 800-115]
Run	A popular, idiomatic expression for program execution. [FISCAM]
Run Manual	A manual that provides application-specific operating instructions, such as instructions on job setup, console and error messages, job checkpoints, and restart and recovery steps after system failures. [FISCAM]

1.1.19 S

Term	Definition
Sabotage	Malicious acts that can cause damage, destruction, interruption, or loss of system assets. This could affect confidentiality, integrity, and availability of data.

Term	Definition
Safeguard	1. A security control or countermeasure employed to reduce the risk associated with a specific threat or group of threats. 2. Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Synonymous with security controls and countermeasures. [FIPS 200]
Salt	A non-secret value that is used in a cryptographic process, usually to ensure that the results of computations for one instance cannot be reused by an attacker.
Sanction	Sanction policies and procedures are actions taken against employees who are non-compliant with security policy.
Sanitize (or Sanitization)	1. The elimination of information from a computer system or media associated with a computer system to permit the reuse of the computer system or media without the possibility that the old information could be accessed and read. 2. The process used to remove information from information system media such that there is reasonable assurance, in proportion to the confidentiality of the information, that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, and destroying media information, prevent the disclosure of organizational information to unauthorized individuals when such media is reused or disposed. [NIST SP 800-53]
Scanning	The process of using software tools to identify hosts, open ports, and provide information on the conditions found.
Scavenging	The process of physical and electronic media searching for remnant (e.g., abandoned or discarded) data that may contain information of value. Physical searching is commonly referred to as “dumpster diving.”
Scenario	A functional exercise staff member who simulates or represents non-participating individuals or organizations whose input or participation is necessary to the flow of the exercise. [NIST SP 800-84]
SDLC Methodology	See System Development Life-Cycle (SDLC).
Section 912	Refers to the “Medicare Prescription Drug, Improvement, and Modernization Act (MMA) of 2003—Sec. 912: Requirements for Information Security for Medicare Administrative Contractors.”
Secure Communication Protocol	A communication protocol that provides the appropriate confidentiality, authentication, and content integrity protection. [NIST SP 800-57]
Secure Name/Address Resolution Service (Recursive or Caching Resolver)	An information system that provides name/address resolution service for local clients and authoritative Domain Name System (DNS) servers are examples of authoritative sources. NIST SP 800-81 provides guidance on secure domain name system deployment. [NIST SP 800-53]

Term	Definition
Secure Name/Address Resolution Service (Authoritative Source)	Enables remote clients to obtain origin authentication and integrity verification assurances for the name/address resolution information obtained through the service. A Domain Name System (DNS) server is an example of an information system that provides name/address resolution service; digital signatures and cryptographic keys are examples of additional artifacts; and DNS resource records are examples of authoritative data. NIST SP 800-81 provides guidance on secure DNS deployment. [NIST SP 800-53]
Secure Shell (SSH)	A program to log-on to another computer over a network, to execute commands in a remote machine, and to move files from one machine to another while providing strong authentication and secure communications over insecure channels. It is intended as a replacement for telnet, rlogin, rsh, and rcp.
Secure Sockets Layer (SSL)	1. A commonly used protocol for managing the security of message transmission on the Internet. Often used in Internet transactions. 2. Protocol based on public key cryptography. Used to generate a cryptographic session that is private to a Web server and a client browser. [NIST SP 800-41]
Security	1. Procedures that protect organizational resources, employees and peers, paper or electronic media, hardware, software and networks from damage, theft, interruption, or change. 2. The protection of computer facilities, computer systems, and data stored on computer systems or transmitted via computer networks from loss, misuse, or unauthorized access. Computer security, as defined by Appendix III to OMB Circular A-130, involves the use of management, personnel, operational, and technical controls to ensure that systems and applications operate effectively and provide confidentiality, integrity, and availability. [FISCAM] 3. A technological discipline concerned with ensuring that information technology (IT) systems perform as expected and do nothing more; that information is provided adequate protection for confidentiality; that system, data and software integrity is maintained; and that information and system resources are protected against unplanned disruptions of processing that could seriously impact mission accomplishments. Also referred to as IT security. [NIST SP 800-16]
Security Accreditation	See Accreditation.
Security Administrator (SA)	Person who is responsible for managing the security program for computer facilities, computer systems, and/or data that is stored on computer systems or transmitted via computer networks. [FISCAM]
Security Assertion Markup Language (SAML)	A specification for encoding security assertions in the extensible markup language (XML).
Security Assessment	The testing and/or evaluation of the management, operational, and technical security controls in an information system 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. [NIST SP 800-53A]

Term	Definition
Security Attribute	A security-related quality of an object. Security attributes may be represented as hierarchical levels, bits in a bit map, or numbers. Compartments, caveats, and release markings are examples of security attributes. [FIPS 188]
Security Authorization (to Operate)	See Authorization to Operate.
Security Authorization Boundary	All components of an information system to be authorized for operation by an authorizing official and excludes separately authorized systems, to which the information system is connected. [NIST SP 800-37]
Security Awareness	1. The general, collective awareness of an organization's personnel on the importance of security and security controls. 2. Awareness is not training. The purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize information technology security concerns and respond accordingly. [NIST SP 800-16] 3. Awareness presentations are intended to allow individuals to recognize information security concerns and respond accordingly. Awareness relies on reaching broad audiences. [NIST SP 800-50]
Security Category	The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, or individuals. [FIPS 199, NIST SP 800-53]
Security Certification	Obsolete. See Security Control Assessment.
Security Clearance	An administrative determination based upon the results of a favorably adjudicated background investigation that an individual is trustworthy and may be granted access to a specified level of classified national security information as required in the performance of assigned duties. [DHHS *Personnel Security/Suitability Handbook*]
Security Communications Protocol	A communication protocol that provides the appropriate confidentiality, authentication, and content integrity protection. [NIST SP 800-57]
Security Control	The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. [FIPS 199]
Security Control Assessment (SCA)	The testing and/or evaluation of the management, operational, and technical security controls in an information system 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. [NIST SP 800-37]
Security Control Assessor	The individual, group, or organization responsible for conducting a security control assessment. [NIST SP 800-37]
Security Control Baseline	The set of minimum security controls defined for a low-impact, moderate-impact, or high-impact information system. [FIPS 200]
Security Control Enhancement	Statements of security capability to: (i) build in additional, but related, functionality to a basic control; and/or (ii) increase the strength of a basic control. [NIST SP 800-53A]

Term	Definition
Security Control Inheritance	A situation in which an information system or application receives protection from security controls (or portions of security controls) that are developed, implemented, and assessed for effectiveness by other entities either internal or external to the organization where the system or application resides. [NIST SP 800-37]
Security Controls Assessment	Synonym of Security Control Assessment (SCA)
Security Domain	1. A scope or environment of trust that shares a single security policy and a single management. 2. A collection of entities to which applies a single security policy executed by a single authority. [FIPS 188]
Security Function	The hardware, software, and firmware of the information system responsible for supporting and enforcing the system security policy and supporting the isolation of code and data on which the protection is based. [NIST SP 800-53A]
Security Impact Analysis	The analysis conducted by an organizational official to determine the extent to which changes to the information system have affected the security state of the system. [NIST SP 800-37, 53, 53A, IR7298]
Security Incident	The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. Security incident also means the loss of data through theft or device misplacement, loss or misplacement of hardcopy documents and misrouting of mail, all of which may have the potential to put the data at risk of unauthorized access, use, disclosure, modification, or destruction.
Security Label	1. Explicit or implicit marking of a data structure or output media associated with an information system representing the FIPS 199 security category, or distribution limitations or handling caveats of the information contained therein. [NIST SP 800-53A] 2. A marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource. [FIPS 188]
Security Level	A hierarchical indicator of the degree of sensitivity to a certain threat. It implies, according to the security policy being enforced, a specific level of protection. [FIPS 188]
Security Level Designation	A rating based on the sensitivity of data (i.e., the need to protect data from unauthorized disclosure, fraud, waste, or abuse) and the operational criticality of data processing capabilities (i.e., the consequences were data processing capabilities to be interrupted for some period of time or subjected to fraud or abuse). There are four security level designations for data sensitivity and four security level designations for operational criticality. The highest security level designation for any data or process within an AIS is assigned for the overall security level designation. [DHHS]

Term	Definition
Security Management Function	1. Computer code intended to repair or lessen the impact of vulnerabilities within application software. 2. The function responsible for the development and administration of an entity's information security program. This includes assessing risks, implementing appropriate security policies and related controls, establishing a security awareness and education program for employees, and monitoring and evaluating policy and control effectiveness. [FISCAM]
Security Objective	Confidentiality, integrity, or availability. [FIPS 199; FIPS 200]
Security Patch	Computer code intended to repair or lessen the impact of vulnerabilities within application software.
Security Plan	Formal document that provides an overview of the security requirements for an information system or an information security program and describes the security controls in place or planned for meeting those requirements. [NIST SP 800-53; SP 800-53A; SP 800-37; SP 800-18] Also see System Security Plan (SSP).
Security Policy	1. The set of laws, rules, and practices that regulates how an organization manages, protects, eliminates, and distributes sensitive information. 2. In business, a security policy is a document that states in writing how a company plans to protect the company's physical and Information Technology assets. A security policy is often considered a "living document", which means that the document is never finished, but is continuously updated as technology and employee requirements change. 3. A senior management directive to create a computer security program, establish its goals, and assign responsibilities. [NIST SP 800-12] 4. A set of criteria for the provision of security services. It defines and constrains the activities of a data processing facility in order to maintain a condition of security for systems and data. [FIPS 188]
Security Profile	See Profile.
Security Program	1. An entity-wide program for security planning and management that forms the foundation of an entity's security control structure and reflects senior management's commitment to addressing security risks. The program should establish a framework and continuing cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of these procedures. [FISCAM] 2. A program established, implemented, and maintained to ensure that adequate information technology (IT) security is provided for all organizational information collected, processed, transmitted, stored, or disseminated in its IT systems. [NIST SP 800-16]
Security Requirement	1. Requirements levied on an information system that are derived from applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, procedures, or organizational mission/business case needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted. [FIPS 200]

Term	Definition
Security Requirements Baseline	Description of the minimum requirements necessary for an information system to maintain an acceptable level of security. [CNSSI 4009]
Security Service	1. A capability that supports one, or many, of the security goals. Examples of security services are key management, access control, and authentication. [NIST SP 800-27A] 2. Mechanism used to provide confidentiality, data integrity, authentication, or non-repudiation of information. [NIST SP 800-57, Part 1]
Security Software	Software that protects data against unauthorized access.
Security Specification	A security specification is a detailed description of the safeguards required to protect a sensitive application (or any automated information system [AIS] asset). [OMB Circular A-130]
Security Tag	Information unit containing a representation of certain security-related information (e.g., a restrictive attribute bit map). [FIPS 188]
Security Test and Evaluation (ST&E)	Obsolete (per 800-37 R1). See Security Controls Assessment.
Security Testing	A process that is used to determine that the security features of a system are implemented and functioning as designed. This process includes hands on functional testing, penetration testing, and verification.
Security Training	1. Security training teaches people the [security] skills that will enable them to perform their jobs more effectively. [NIST SP 800-16] 2. Training strives to produce relevant and needed security skills and competencies. [NIST SP 800-50] Also see Security Awareness.
Sensitive Application	1. An application that processes sensitive data. 2. An application of information technology that requires protection because it processes sensitive data, or because of the risk and magnitude of loss or harm that could result from improper operation, deliberate manipulation, [or delivery interruption] of the application. [OMB Circular A-130]
Sensitive But Unclassified (SBU) Information	The categorization of information whose exposure could prove detrimental to a system, person, or organization but will not create serious damage to national security if disclosed. Health care information is an example of SBU data.
Sensitive Data	1. Data that require protection due to the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the data. The term includes data whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary data, records about individuals requiring protection under the Privacy Act, and data not releasable under the Freedom of Information Act. [OMB Circular A-130] 2. 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. [FIPS 102]

Term	Definition
Sensitive Information	1. Data, which the loss, misuse, or unauthorized access to or modification of, could adversely affect national interest, the conduct of federal programs, or the privacy to which individuals are entitled under 5 USC Sec. 552a (the Privacy Act), but that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. 2. Any information that, if lost, misused, or accessed or modified in an improper manner, could adversely affect the national interest, the conduct of federal programs, or the privacy to which individuals are entitled under the Privacy Act. [FISCAM] 3. Information that requires protection due to the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information. The term includes information whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary information, records about individuals requiring protection under the Privacy Act, and information not releasable under the Freedom of Information Act. [NIST SP 800-26] 4. Any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under section 552a of title 5, USC (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. [Computer Security Act of 1987]
Sensitive Media	Any form in which sensitive information is stored including paper, diskette, etc.
Sensitivity	The degree to which an information technology system or application requires protection (to ensure confidentiality, integrity, and availability) which is determined by an evaluation of the nature and criticality of the data processed, the relation of the system to the organization missions and the economic value of the system components. [NIST SP 800-16]
Sensitivity Level	A graduated system of marking (e.g., low, moderate, high) information and information processing systems based on threats and risks that result if a threat is successfully conducted. [FIPS 201]
Separation of Duty/Segregation of Duty	To ensure that no single person has control of a transaction from beginning to end and that two or more people are responsible for its execution. This is intended to prevent one person from manipulating transactions for personal gain.
Server	1. A network device that provides service to the network users by managing shared resources. Note: This term is often used in the context of client-server architecture for a local area network. 2. A computer running administrative software that controls access to all or part of the network and its resources, such as disk drives or printers. A computer acting as a server makes resources available to computers acting as workstations on the network. [FISCAM]
Service Continuity Control	This type of control involves ensuring that when unexpected events occur, critical operations continue without interruption or are promptly resumed and critical and sensitive data are protected. [FISCAM]

Term	Definition
Session	A session is an encounter between an end-user interface device (e.g., computer, terminal, process) and an application, including a network logon. One user session is the time between starting the application and quitting. [Adapted from multiple sources]
Session Control	The application of security mechanisms to network connections which are intended to prevent unauthorized persons from capturing or modifying network connection data, or taking control of pre-established network connections.
Severity of Impact	The degree of potential loss of confidentiality, integrity, and/or system availability.
Shared Secret	A secret used in authentication that is known only to the claimant and the verifier. [NIST SP 800-63]
Shoulder Surfing	The capture via observation of information as it is entered by authorized personnel (e.g., stealing phone numbers or passwords).
Shred	A method of sanitizing media; the act of cutting or tearing into small particles. [NIST SP 800-88]
Signature	A recognizable, distinguishing pattern associated with an attack, such as a binary string in a virus or a particular set of keystrokes used to gain unauthorized access to a system. [NIST SP 800-61]
Signature Certificate	A public key certificate that contains a public key intended for verifying digital signatures rather than encrypting data or performing any other cryptographic functions. [NIST SP 800-32]
Signature Verification	Uses a digital signature algorithm and a public key to verify a digital signature. [NIST SP 800-57]
Signed Data	Data on which a digital signature is generated. [FIPS 196]
Significant Change	1. A change that is likely to affect the security state of an information system. [NIST SP 800-37 R1] 2. Examples of significant changes to an information system may include: (i) installation of a new or upgraded operating system, middleware component, or application; (ii) modifications to system ports, protocols, or services; (iii) installation of a new or upgraded hardware platform; (iv) modifications to cryptographic modules or services; or (v) modifications to security controls. Examples of significant changes to the environment of operation may include for example: (i) moving to a new facility; (ii) adding new core missions or business functions; (iii) acquiring specific and credible threat information that the organization is being targeted by a threat source; or (iv) establishing new/modified laws, directives, policies, or regulations. 3. The examples of changes listed above are only significant when they meet the threshold established in the definition of significant change (i.e., a change that is likely to affect the security state of the information system).

Term	Definition
Single Loss Expectancy (SLE)	This value, classically, is derived from the following algorithm to determine the monetary loss (impact) for each occurrence of a threatened event: ASSET VALUE x EXPOSURE FACTOR = SLE The SLE is usually a result of a business impact analysis (BIA). A BIA typically stops short of evaluating the related threats' Annualized Rate of Occurrence (ARO) or its significance. The SLE represents only one element of risk, the expected impact, monetary or otherwise, of a specific threat event. Because the BIA usually characterizes the massive losses resulting from a catastrophic event, however improbable, it is often employed as a scare tactic to get management attention and loosen budgetary constraints.
Smart Card	1. Small object similar to a credit card containing a chip with logic functions and information that can be "read" at a remote terminal to identify the holder's personal data or access privileges. The card contains pre-recorded, usually encrypted access control information that is verified against data that the user provides, such as a personal identification number (PIN). 2. A credit card with a built-in microprocessor and memory that is used for identification or financial transactions. When inserted into a reader, the card transfers data to and from a central computer. A smart card is more secure than a magnetic stripe card and can be programmed to self-destruct if the wrong password is entered too many times. [NIST SP 800-48]
Sniffer	Synonymous with packet "sniffer". A program that intercepts routed data and examines each packet in search of specified information, such as passwords transmitted in clear text. [FISCAM] Also see Packet Sniffer.
Social Engineering	1. Social engineering is the technique of using persuasion and/or deception to gain access to, or information about, information systems. Typically, it is implemented through human conversation or other interaction. The usual medium of choice is telephone but can also be e-mail or even face-to-face interaction. 2. An attempt to trick someone into revealing information (e.g., a password) that can be used to attack systems or networks. [NIST SP 800-61]
Software	The computer program that instructs computer hardware to perform an action. System software is the operating system that controls the basic functioning capabilities of the computer, network software enables multiple computers to communicate with one another, and language software is used to develop programs.
Software Assurance	The level of confidence that software is free from vulnerabilities, either inadvertently designed into the software or accidentally inserted at any time during its lifecycle, and that the software functions in the intended manner. [CNSS Inst. 4009, National Information Assurance (IA) Glossary, April 26, 2010 US-CERT IT Security EBK: A Competency and Functional Framework]

Term	Definition
Software Life-Cycle	The phases in the life of a software product, beginning with its conception and ending with its retirement. These stages generally include requirements analysis, design, construction, testing (validation), installation, operation, maintenance, and retirement. [FISCAM]
Software Security	General purpose (executive, utility, or software development tools) and applications programs or routines that protect data handled by a system. [NCSC-TG-004]
Source Code	Human-readable program statements written in a high-level or assembly language, as opposed to object code, which is derived from source code and designed to be machine-readable. [FISCAM]
Special Management Attention	Some systems require "special management attention" to security due to the risk and magnitude of the harm that would result from the loss, misuse, unauthorized access to, or modification of the information in the system. [OMB Circular A-130]
Specification	An assessment object that includes document-based artifacts (e.g., policies, procedures, plans, system security requirements, functional specifications, and architectural designs) associated with an information system. [NIST SP 800-53A]
Spoofing	1. An attack in which an unauthorized person or process pretends to be an authorized person or process. 2. Refers to sending a network packet that appears to come from a source other than its actual source. [NIST SP 800-48]
Spyware	Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge; a type of malicious code. [NIST SP 800-53]
Stand-alone System (or Computer)	A system that does not require support from other devices or systems. Links with other computers, if any, are incidental to the system's chief purpose. [FISCAM]
Standard	1. A standard can be: • An object or measure of comparison that defines or represents the magnitude of a unit; • A characterization that establishes allowable tolerances or constraints for categories of items; or • A degree or level of required excellence or attainment. 2. Standards are definitional in nature, established either to further understanding and interaction, or to acknowledge observed (or desired norms) of exhibited characteristics or behavior. For the purposes of CMS, an information technology standard is an officially categorized convention, methodology, or preferred product authorized for use within CMS. 3. A published statement on a topic specifying characteristics, usually measurable, that shall be satisfied or achieved in order to comply with the standard. [FIPS 201] 4. In computing, a set of detailed technical guidelines used as a means of establishing uniformity in an area of hardware or software development. [FISCAM] Also see Implementation Standard.

Term	Definition
Standard Profile	A set of rules that describes the nature and extent of access to each resource that is available to a group of users with similar duties, such as accounts payable clerks. [FISCAM]
Storage	Retrievable retention of data. Electronic, electrostatic, or electrical hardware or other elements (media) into which data may be entered, and from which data may be retrieved. [NIST SP 800-88]
Storage Security	The process of allowing only authorized parties to access stored information. [NIST SP 800-111]
Subject	The person whose identity is bound in a particular credential. [NIST SP 800-63]
Subscriber	A party who receives a credential or token from a CSP and becomes a claimant in an authentication protocol.
Subsystem	A major subdivision or component of an information system consisting of information, information technology, and personnel that perform one or more specific functions. [NIST SP 800-18]
Suitability	Refers to identifiable character traits and conduct sufficient to decide whether an individual is likely or not likely to be able to carry out the duties of a federal job with appropriate integrity, efficiency, and effectiveness. Suitability is distinguishable from a person's ability to fulfill the qualification requirements of a job, as measured by experience, education, knowledge, and skills. [OPM]
Symbolic Link	A symbolic link (symlink or soft link) is a special type of file that points to another directory or file inside an operating system.
Symmetric Encryption Algorithm	Encryption algorithms using the same secret key for encryption and decryption. [NIST SP 800-49]
Symmetric Key	A cryptographic key that is used to perform both the cryptographic operation and its inverse (i.e., to encrypt and decrypt, or create a message authentication code and to verify the code). [NIST SP 800-63]

Term	Definition
System	1. A system normally includes hardware, software, information, data, applications, telecommunication systems, network communications systems, and people. A system's hardware may include mainframe systems, desktop systems (e.g., personal computers, Macintoshes, laptops, handheld devices), workstations and servers (e.g., UNIX, NT), local area networks (LANs), and any other platform regardless of the operating system (OS). 2. A set of information resources under the same management control that share common functionality and require the same level of security controls. 3. The phase "General Support Systems" (GSSs) as used in OMB Circular A-130, Appendix III, is replaced in this document with "system" for easy readability. A "system" includes "Major Applications" (MAs), as used in OMB Circular A-130, Appendix III, (e.g., payroll and personnel program software, control software, or software for command and control). 4. By categorizing both "General Support Systems" and "Major Applications" as "systems", unless explicitly stated, the procedures and guidance can address both in a simplified manner. 5. When writing the required System Security Plans, two formats are provided--one for GSSs, and one for MAs. This ensures that the differences for each are addressed. 6. An interconnected set of information resources under the same direct management control, which shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people. [OMB Circular A-130] 7. A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. [NIST SP 800-53] Also see Information System.
System Administrator	1. A person who manages the technical aspects of a system. [NIST SP 800-40) 2. The person responsible for administering use of a multi-user computer system, communications system, or both. [FISCAM]
System Analyst	A person who examines the logic, functions, and performance of a system to determine its applicability and effectiveness for a purpose, or its security. [FISCAM]
System Backup	See Backup.
System Basic Input/Output System (BIOS)	See Basic Input/Output System (BIOS).

Term	Definition
System Development Life-Cycle (SDLC)	1. The system life-cycle is the period of time beginning when the software product is conceived and ending when the resultant software products are no longer available for use. The SDLC, typically, is broken into phases, such as requirements, design, programming and testing, installation, and operations and maintenance. Each phase consists of a well-defined set of activities whose products lead to the evolution of the activities and products of each successive phase. 2. The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal that instigates another system initiation. [NIST SP 800-34] 3. The policies and procedures that govern software development and modification as a software product goes through each phase of its life-cycle. [FISCAM]
System Environment	The operational characteristics and layout of a system, including purpose, application, and configuration.
System Event Auditing	The process of identifying, detecting, and logging a set of pre-defined system and user activities.
System Identification	Documentation of the name, purpose, configuration and organization responsible for a General Support System (GSS), Major Application (MA), or "Other" system.
System Impact	The degree of harm or potential harm caused to a system.
System Integrity	The quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation of the system, whether intentional or accidental. [NIST SP 800-27A]
System Interconnection/ System Sharing	The direct connection of two or more information technology systems for sharing data and other information resources. [NIST SP 800-47]
System Interface	A shared boundary where interaction occurs; i.e., the boundary between two or more subsystems or devices.
System Life-Cycle	The period beginning when the software product is conceived and ending when the resultant software products are no longer available for use. The system life-cycle, typically, is broken into phases, such as requirements, design, programming and testing, installation, and operations and maintenance. Each phase consists of a well-defined set of activities whose products lead to the evolution of the activities and products of each successive phase. [FIPS 101] Also see Software Life-Cycle.
System Maintainer	The individual or group of individuals who have the responsibilities of continued maintenance (e.g., bug fixing, minor modifications/ enhancements, performance tuning, and/or customer service) of an implemented system. A system maintainer may or may not also serve as the system developer for a given project.
System Management Facility	An IBM control program that provides the means for gathering and recording information that can be used to evaluate the extent of computer system usage. [FISCAM]

Term	Definition
System Media	Includes both digital media (e.g., diskettes, magnetic tapes, external/ removable hard drives, flash/thumb drives, compact disks [CD], digital video disks [DVD]) and non-digital media (e.g., paper, microfilm). [NIST SP 800-53]
System Operational Status	• New: The status of a development effort with the objective of producing a system that has not previously been implemented. • Operational: The status of a system currently supporting a CMS business function or meeting a CMS business need. • Undergoing major modification: The status of a system supporting a CMS business function or meeting a CMS business need that is subject to changes in its functionality or information security controls.
System Outage	An unplanned interruption in system availability as a result of computer hardware or software problems, or operational problems.
System Owner/Manager	See Business Owner.
System Programmer	A person who develops and maintains system software. [FISCAM]
System Security	Refers to the concepts, techniques, technical measures, and administrative measures used to protect the hardware, software, and data of an information processing system from deliberate or inadvertent unauthorized acquisition, damage, destruction, disclosure, manipulation, modification, use, or loss. [FIPS 11-3]
System Security Administrator (SSA)	The person responsible for administering security on a multi-user computer system, communications system, or both.
System Security Incident (Breach)	Those incidents not classified as physical crimes, criminal violations, fraudulent activity, illegal access and disclosure or misuse of government property. A systems security breach is any action involving a system, which, if not corrected, could violate the provisions of the Privacy Act, Copyright laws, or CMS security policy or lead to a fraudulent act or criminal violation through use of a CMS system. Also see Breach.
System Security Officer (SSO)	The position held by the business partner security officer with complete oversight and responsibility for all aspects of the security of the Medicare program.
System Security Plan (SSP)	1. Formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements. [FIPS 200; NIST SP 800-37; SP 800-53; SP 800-53A; SP 800-18]
System Security Profile	Detailed security description of the physical structure, equipment component, location, relationships, and general operating environment of an information system. [CNSSI 4009]

Term	Definition
System Software	1. The special software within the cryptographic boundary (e.g., operating system, compilers or utility programs) designed for a specific computer system or family of computer systems to facilitate the operation and maintenance of the computer system, and associated programs, and data. [FIPS 140-2] 2. The set of computer programs and related routines designed to operate and control the processing activities of computer equipment. It includes the operating system and utility programs and is distinguished from application software. [FISCAM]
System Test	1. A test performed on a complete system to evaluate its compliance with specified requirements. [NIST SP 800-84] 2. Testing to determine that the results generated by the enterprise's information systems and their components are accurate and the systems perform to specification. [FISCAM]
Systems Security Coordinator (SSC)	Term used to designate the security officer in the 1992 Regional Office Manual (ROM), Medicare Intermediary Manual (MIM), and Medicare Carriers Manual (MCM). This Business Partner security officer had complete oversight and responsibility for all aspects of the security of the Medicare program.
System-specific Security Control	A security control for an information system that has not been designated as a common security control or the portion of a hybrid control that is to be implemented within an information system. [NIST SP 800-37 R1]

1.1.20 T

Term	Definition
Tabletop Exercise	A discussion-based exercise where personnel with roles and responsibilities in a particular information technology plan meet in a classroom setting or in breakout groups to validate the content of the plan by discussing their roles during an emergency and their responses to a particular emergency situation. A facilitator initiates the discussion by presenting a scenario and asking questions based on the scenario. [NIST SP 800-84]
Tailoring	The process by which a security control baseline selected in accordance with the FIPS 199 security categorization of the information system is modified based on: • The application of scoping guidance; • The specification of compensating security controls, if needed; and • The specification of organization-defined parameters in the security controls, where allowed. [NIST SP 800-53A]
Tampering	An unauthorized modification that alters proper functioning of equipment or systems in a manner that degrades security or functionality.
Tape Library	The physical site where magnetic media is stored. [FISCAM]
Tape Management System	Software that controls and tracks tape files. [FISCAM]

Term	Definition
Technical Control	The security controls (i.e., safeguards or countermeasures) for 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. [FIPS 200]
Technical Safeguard	The technology and the policy and procedures for its use that protect electronic protected health information and control access to it. [HIPAA]
Telecommunications	1. The transmission, between or among points specified by the user, of information of the user's choosing, without change in the form or content of the information as sent and received. [NIST SP 800-60 Vol. 2] 2. A general term for the electronic transmission of information of any type, such as data, television pictures, sound, or facsimiles, over any medium, such as telephone lines, microwave relay, satellite link, or physical cable. [FISCAM]
Tempest	A name referring to the investigation, study, and control of unintentional compromising emanations from telecommunications and automated information systems equipment. [FIPS 140-2]
Terminal	A device consisting of a video adapter, a monitor, and a keyboard. [FISCAM]
Terrorism	A deliberate and violent act taken by an individual or group whose motives go beyond the act of sabotage, generally toward some political or social sentiment/position.
Test	A type of assessment method that is characterized by the process of exercising one or more assessment objects under specified conditions to compare actual with expected behavior, the results of which are used to support the determination of security control effectiveness over time. [NIST SP 800-53A]
Test Bed	Test environment containing the software, data, and simulations necessary for testing systems.
Test Plan	A document that outlines the specific steps that will be performed for a particular test, including the required logistical items and expected outcome or response for each step. [NIST SP 800-84]
Threat	1. Any circumstance or event that has the potential to cause harm to a system (whether intentional or unintentional) in the form of destruction, disclosure, modification of data, interruption, and/or denial of service. 2. Any circumstance or event with the potential to adversely impact agency operations (including mission, functions, image, or reputation), agency assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. [NIST SP 800-53]
Threat Agent	See Threat Source.
Threat Analysis	The examination of threat sources against system vulnerabilities to determine the threats for a particular system in a particular operational environment. [NIST SP 800-27A]
Threat Assessment	Formal description and evaluation of threat to an information system. [NIST SP 800-53; CNSSI 4009]

Term	Definition
Threat Source	1. The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability. [FIPS 200] 2. Either: a. Intent and method targeted at the intentional exploitation of a vulnerability; or b. A situation and method that may accidentally trigger a vulnerability. Synonymous with threat agent. [NIST SP 800-37]
Token	1. A physical device used to convey privilege or a capability (e.g., a handheld password generator). 2. In authentication systems, some type of physical device (such as a card with a magnetic strip or a smart card) that must be in the individual's possession in order to gain access. The "token" itself is not sufficient; the user must also be able to supply something memorized, such as a personal identification number (PIN). [FISCAM] 3. Something that the claimant possesses and controls (typically a key or password) used to authenticate the claimant's identity. [NIST SP 800-63]
Topology	The physical, non-logical features of a card. A card may have either standard or enhanced topography. [FIPS 201]
Top Secret	The highest level of information classification. The unauthorized disclosure of top-secret information will cause exceptionally great damage to the country's national security.
Tracking Cookie	A cookie placed on a user's computer to track the user's activity on different Web sites, creating a detailed profile of the user's behavior. [NIST SP 800-83]
Training (Information Security)	1. Training in organizational policies and procedures, security requirements, legal responsibilities, business controls, and correct, safe use of information processing facilities. 2. Teaching people the knowledge and skills that will enable them to perform their jobs more effectively. [NIST SP 800-16] 3. Training strives to produce relevant and needed (information) security skills and competencies. [NIST SP 800-50] Also see Awareness (Information Security).
Transaction	A discrete activity captured by a computer system, such as an entry of a customer order or an update of an inventory item. In financial systems, a transaction generally represents a business event that can be measured in money and entered in accounting records. [FISCAM]
Transaction File	A group of one or more computerized records containing current business activity and processed with an associated master file. Transaction files are sometimes accumulated during the day and processed in batch production overnight or during off-peak processing periods. [FISCAM]

Term	Definition
Transport Layer Security (TLS)	1. An authentication and security protocol widely implemented in browsers and web servers. TLS is defined by [RFC 2246] and [RFC 3546]. TLS is similar to the older Secure Sockets Layer (SSL) protocol and is effectively SSL version 3.1. 2. While SSL 3.0 is the most secure of the SSL protocol versions, it is not approved for use in the protection of federal information because it relies in part on the use of cryptographic algorithms that are not FIPS-approved. TLS, when properly configured, is approved for the protection of federal information. [NIST SP 800-52]
Trap Door	A hidden software or hardware mechanism that can be triggered to permit system protection mechanisms to be circumvented. It is activated in some innocent-appearing manner; e.g., a special "random" key sequence at a terminal. Software developers often introduce trap doors in their code to enable them to re-enter the system and perform certain functions. Synonymous with back door. [NCSC-TG-004]
Triple Data Encryption Algorithm (TDEA) (aka Triple DES)	An implementation of the Data Encryption Standard (DES) algorithm that uses three passes of the DES algorithm instead of one as used in ordinary DES applications. Triple DES provides much stronger encryption than ordinary DES but it is less secure than Advanced Encryption Standard (AES). [NIST SP 800-46] Note: Through the year 2030, TDEA and AES will coexist as FIPS-approved algorithms–thus, allowing for a gradual transition to AES. Also see Triple Data Encryption Standard (Triple DES).
Triple Data Encryption Standard (Triple DES)	Triple DES is recognized as the only FIPS-approved Data Encryption Standard (DES) algorithm. Other implementations of the DES function are no longer authorized for protection of federal government information. [NIST SP 800-67] Note: Through the year 2030, Triple Data Encryption Algorithm (TDEA) and Advanced Encryption Standard (AES) will coexist as FIPS-approved algorithms–thus, allowing for a gradual transition to AES.
Trojan Horse	1. A computer program with an apparent or actual useful function that contains additional, malicious, and hidden functions. 2. A non-self-replicating program that seems to have a useful purpose, but in reality has a different, malicious purpose. [NIST SP 800-61]
Trusted Agent	Entity authorized to act as a representative of an agency in confirming Subscriber identification during the registration process. Trusted Agents do not have automated interfaces with Certification Authorities. [NIST SP 800-32]
Trusted Certificate	A certificate that is trusted by the Relying Party based on secure and authenticated delivery. The public keys included in trusted certificates are used to start certification paths. Also known as a "trust anchor". [NIST SP 800-32]

Term	Definition
Trusted Path	1. A mechanism by which a user (through an input device) can communicate directly with the security functions of the information system with the necessary confidence to support the system security policy. This mechanism can be activated only by the user or the security functions of the information system and cannot be imitated by untrusted software. [NIST SP 800-53A] 2. A means by which an operator and a target of evaluation security function can communicate with the necessary confidence to support the target of evaluation security policy. [FIPS 140-2]
Trustworthiness	A characteristic or property of an information system that expresses the degree to which the system can be expected to preserve the confidentiality, integrity, and availability of the information being processed, stored, or transmitted by the system. [NIST SP 800-39]
Tunneled Password Protocol	A protocol where a password is sent through a protected channel. For example, the Transport Layer Security (TLS) protocol is often used with a verifier's public key certificate to: • Authenticate the verifier to the claimant; • Establish an encrypted session between the verifier and claimant; and • Transmit the claimant's password to the verifier. The encrypted TLS session protects the claimant's password from eavesdroppers. [NIST SP 800-63]
Two-Factor Authentication	A type of authentication that requires two independent methods to establish identity and authorization to perform services. The three most recognized factors are: • "Something you are" (e.g., biometrics) • "Something you know" (e.g., password) • "Something you have" (e.g., smart card) [FIPS 140-3]

1.1.21 U

Term	Definition
Unauthorized Access	1. Occurs when a user, legitimate or unauthorized, accesses a resource that the user is not permitted to use. [FIPS 191] 2. A person gains logical or physical access without permission to a network, system, application, data, or other IT resource. [NIST SP 800-61]
Unauthorized Disclosure	An event involving the exposure of information to entities not authorized access to the information. [NIST SP 800-57]
Uncertainty	This term characterizes the degree, expressed as a percent, from 0.0 to 100%, to which there is less than complete confidence in the value of any element of the risk assessment. Uncertainty is typically measured inversely with respect to confidence (i.e., if confidence is low, uncertainty is high).

Term	Definition
Unclassified	1. Information that is designated as neither sensitive nor classified. The public release of this information does not violate national security interests. 2. Information that has not been determined pursuant to E.O. 12958 or any predecessor order to require protection against unauthorized disclosure and that is not designated as classified. [CNSSI 4009]
Universal Serial Bus (USB)	A hardware interface for low-speed peripherals such as the keyboard, mouse, joystick, scanner, printer, and telephony devices. [NIST SP 800-124]
UNIX	A multitasking operating system originally designed for scientific purposes, which has subsequently become a standard for midrange computer systems with the traditional terminal/host architecture. UNIX is also a major server operating system in the client/server environment. [FISCAM]
Unsigned Data	Data included in an authentication token, in addition to a digital signature. [FIPS 196]
Update Access	This access level includes the ability to change data or a software program. [FISCAM]
User	1. Individual or (system) process authorized to access an information system. [FIPS 200; NIST SP 800-53; CNSSI 4009] 2. Any organizational or programmatic entity that [utilizes or] receives service from an [automated information system] facility. A user may be either internal or external to the agency organization responsible for the facility, but normally does not report to either the manager or director of the facility or to the same immediate supervisor. [OMB Circular A-130] 3. The person who uses a computer system and its application programs to perform tasks and produce results. [FISCAM] 4. An individual or process (subject) acting on behalf of the individual that accesses a cryptographic module in order to obtain cryptographic services. [FIPS 140-2]
User Account Management	Focuses on identification, authentication, and access authorizations. Involves: • The process of requesting, establishing, issuing, and closing user accounts; • Tracking users and their respective access authorizations; and • Managing these functions. [NIST SP 800-12]
User Identification (UserID)	A unique identifier assigned to each authorized computer user. [FISCAM]
User Profile	A set of rules that describes the nature and extent of access to each resource that is available to each user. [FISCAM]
User Registration	A stage in the lifecycle of keying material; a process whereby an entity becomes a member of a security domain. [NIST SP 800-57]
Utility Program	Generally considered to be system software designed to perform a particular function (e.g., an editor or debugger) or system maintenance (e.g., file backup and recovery). [FISCAM]

1.1.22 V

Term	Definition
Valid Data Element	A payload, an associated data string, or a nonce that satisfies the restrictions of the formatting function. [NIST SP 800-38C]
Validation	The process of demonstrating that the system under consideration meets in all respects the specification of that system. [FIPS 201]
Validation Control	1. Controls, tests, and evaluations that assess the level of compliance with security specifications and requirements. 2. The process of evaluating a system or component during or at the end of the development process to determine whether it satisfies specified requirements. [FISCAM]
Verification	The process of affirming that a claimed identity is correct by comparing the offered claims of identity with previously proven information stored in the identity card or Personal Identity Verification (PIV) system. [FIPS 201] Also see Identity Verification.
Verified Name	A subscriber name that has been verified by identity proofing. [NIST SP 800-63]
Verifier	An entity that verifies the claimant's identity by verifying the claimant's possession of a token using an authentication protocol. To do this, the verifier may also need to validate credentials that link the token and identity and check their status. [NIST SP 800-63]
Victim	A machine that is attacked. [NIST SP 800-61]
Virtual Private Network (VPN)	1. A combination of tunneling, encryption, authentication, and access control technologies and services used to carry traffic over the Internet, a managed Internet protocol (IP) network, or a provider's backbone network to ensure the security of information transmitted. 2. A virtual private network is a logical network that is established, at the application layer of the Open Systems Interconnection (OSI) Model, over an existing physical network and typically does not include every node present on the physical network. [NIST SP 800-46] 3. A virtual network, built on top of existing physical networks, which can provide a secure communications mechanism for data and other information transmitted between networks. [NIST SP 800-113]
Virus	1. A sequence of code inserted into other executable code so that when those programs are run, the viral code is also executed. Viruses reproduce themselves by attaching to other programs. 2. A virus is a program that infects computer files (usually other executable programs) by inserting in those files copies of itself. This is usually done in such a manner that the copies will be executed when the file is loaded into memory, allowing them to infect still other files, and so on. Viruses often have damaging side effects, sometimes intentionally, sometimes not. 3. A self-replicating program that runs and spreads by modifying other programs or files. [NIST SP 800-61]

Term	Definition
Virus Scanning	The process employed by anti-virus software to check for, identify, isolate, and eradicate viruses, Trojan Horses, worms, and other forms of malicious code.
Volatile Memory	Memory that loses its content when power is turned off or lost. [NIST SP 800-124]
Volume	A logical unit of storage comprising a file-system. [NIST SP 800-111]
Volume Encryption	The process of encrypting an entire volume and permitting access to the data on the volume only after proper authentication is provided. [NIST SP 800-111]
Vulnerability	1. A weakness in system security procedures, system design, implementation, controls, and/or configurations that could be breached to violate system security policy. 2. A weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. [FIPS 200; NIST SP 800-53]
Vulnerability Analysis	Systematic examination of systems and applications in order to determine the adequacy of security measures, identify security deficiencies, and provide data from which to predict the effectiveness of proposed security measures.
Vulnerability Assessment	1. A measurement of vulnerability that includes the susceptibility of a particular system to a specific attack and the opportunities available to a threat agent to mount that attack. 2. Formal description and evaluation of the vulnerabilities in an information system. [NIST SP 800-53; CNSSI 4009]
Vulnerability Scanning	A technique used to identify hosts/host attributes and associated vulnerabilities. [NIST SP 800-115]

1.1.23 W

Term	Definition
Warm Site	An environmentally conditioned workspace that is partially equipped with information technology (IT) and telecommunications equipment to support relocated IT operations in the event of a significant disruption. [NIST SP 800-34]
Warning Banner	A notice presented prior to authentication to an access-restricted system identifying the system as a non-public resource, warning that unauthorized access can result in legal persecution and stating that only authorized users are permitted to access the system.
Wide Area Network (WAN)	1. A group of computers and other devices dispersed over a wide geographical area and connected by communications links. [FISCAM] 2. A communications network that connects geographically separated areas. [Microsoft Press Computer Dictionary]
Wired Equivalent Privacy (WEP)	A security protocol for wireless local area networks (WLANs) defined in the 802.11b standard. WEP was intended to provide the same level of security as that of a wired LAN. [NIST SP 800-46]

Term	Definition
Wireless Application Protocol (WAP)	A standard for providing cellular telephones, pagers, and other handheld devices with secure access to email and text-based Web pages. [NIST 800-48]
Wireless Fidelity (Wi-Fi)	A term describing a wireless local area network that observes the IEEE 802.11 protocol. [NIST SP 800-124]
Workaround	A configuration change to a software package or other information technology (IT) resource that mitigates the threat posed by a particular vulnerability. The workaround usually does not fix the underlying problem (unlike a patch) and often limits functionality within the IT resource. [NIST SP 800-40]
Workstation	1. A microcomputer or terminal connected to a network. It can also refer to a powerful, stand-alone computer with considerable calculating or graphics capability. [FISCAM] 2. An electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment. [HIPAA]
Worm	1. An independent program that reproduces by copying itself from one system to another while traveling from machine to machine across network connections. 2. A self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself. [NIST SP 800-61] 3. A program that propagates itself across computers, usually by spawning copies of itself in each computer's memory. A worm might duplicate itself in one computer so often that it causes the computer to crash. Sometimes written in separate segments, a worm is introduced surreptitiously into a host system either for fun or with intent to damage or destroy information. [Microsoft Press Computer Dictionary]
Write	Fundamental operation in an information system that results only in the flow of information from a subject to an object. [CNSSI 4009]
Write Access	Permission to write to an object in an information system. [CNSSI 4009]

1.1.24 X

Term	Definition
X.509 Certificate	The International Organization for Standardization/International Telecommunication Union - Standardization Department (ISO/ITU-T) X.509 standard defined two types of certificates–the X.509 public key certificate, and the X.509 attribute certificate. Most commonly (including this document), an X.509 certificate refers to the X.509 public key certificate. [NIST SP 800-57]

1.1.25 Z

Term	Definition
Zero Knowledge Password	Strong password used with special "zero knowledge" protocol.

Term	Definition
Zero Knowledge Protocol	With “zero-knowledge protocols,” someone can convince the verifier that s/he is in possession of the secret without revealing the secret itself, unlike normal username-password queries.
Zeroization	A method of erasing electronically stored data and cryptographic keys by altering or deleting the contents of the data storage to prevent recovery of the data. [Adapted from FIPS 140-2]
Zombie	A program that is installed on a system to cause it to attack other systems. [NIST SP 800-83]

1.2 ACRONYMS

This section contains acronyms in common use at CMS regarding Information Security. The acronyms are drawn from internal CMS documents, as well as from Federal government, industry, and other external sources to provide a comprehensive resource for the CMS environment.

The alphabetical tables of acronyms begin on the next page.

1.2.1 A

Acronym	Term
A&A	Assessment and Authorization
AAL	Authorized Access List
ABMAC	A/B Medicare Administrative Contractor
AC	Alternating Current
ACL	Access Control List
ADM	Administrative
ADP	Automated Data Processing
AES	Advanced Encryption Standard
AFE	Annual Frequency Estimate
AIE	Annual Impact Estimate
AIS	Automated Information System
ALE	Annual Loss Expectancy
ANSI	American National Standards Institute
APF	Authorized Program Facility
APO	Army Post Office
ARO	Annualized Rate of Occurrence
ARS	Acceptable Risk Safeguards
ASC	Accredited Standards Committee
ATA	Advanced Technology Attachment
ATO	Authorization to Operate

1.2.2 B

Acronym	Term
BCA	Business Case Analysis
BCCP	Business Continuity and Contingency Plan
BCP	Business Continuity Plan
BI	Background Investigation
BIA	Business Impact Analysis
BIOS	Basic Input/Output System
BPSSM	Business Partners Systems Security Manual
BRP	Business Recovery/Resumption Plan

1.2.3 C

Acronym	Term
C&A	Certification and Accreditation (Obsolete [per 800-37 R1], see A&A)

Acronym	Term
CA	Certification Authority
CAP	Corrective Action Plan
CBT	Computer-based Training
CCB	Configuration (or Change) Control Board
CCMO	Consortium Contractor Management Officer
CCP	Common Control Provider
CD	Compact Disc (or Disk)
CD-ROM	Compact Disc-Read-Only Memory
CFACTS	CMS FISMA Control Tracking System
CFR (or C.F.R.)	Code of Federal Regulations
CIA	Confidentiality, Integrity, and Availability
CICG	Critical Infrastructure Coordination Group
CIO	Chief Information Officer
CIRC	Computer Incident Response Center, or Computer Incident Response Capability
CIRT	Computer Incident Response Team
CISO	Chief Information Security Officer
CM	Configuration Management
CMP	Configuration Management Plan
CMS	Centers for Medicare & Medicaid Services
CMSR	CMS Minimum Security Requirements
CNSSI	Committee on National Security Systems Instruction
CO	Central Office, or Contracting Officer
COMSEC	Communications Security
COOP	Continuity of Operations Plan
COTR	Contracting Officer's Technical Representative
COTS	Commercial Off-the-Shelf
CP	Contingency Plan
CPS	Certification Practice Statement
CPU	Central Processing Unit
CRC	Cyclic Redundancy Checks
CRL	Certificate Revocation list
CSAT	Computer Security Awareness Training
CSIRC	Computer Security Incident Response Capability
CSIRT	Computer Security Incident Response Team
CSP	Credentials Service Provider, or Customer Service Plan, or Cloud Service Provider

Acronym	Term
CSR	Core Security Requirements (replaced by CMSRs)
CSS	Cross-Site Scripting
CSSP	Computer Systems Security Plan
CVE	Common Vulnerabilities and Exposures
CWF	Common Working File

1.2.4 D

Acronym	Term
DAA	Designated Approving Authority
DAC	Discretionary Access Control
DASD	Direct Access Storage Devices
DBA	Database Administrators
DBM	Database Management
DBMS	Database Management System
DC	District of Columbia
DCII	Defense Clearance and Investigations Index
DDoS (or DDOS)	Distributed Denial Of Service
DEA	Data Encryption Algorithm
DES	Data Encryption Standard
DHHS	Department of Health and Human Services
DMEMAC	Durable Medical Equipment Medicare Administrative Contractor
DMERC	Durable Medical Equipment Regional Carrier
DMZ	Demilitarized Zone
DNS	Domain Name System
DoS (or DOS)	Denial of Service
DRP	Disaster Recovery Plan
DSL	Digital Subscriber Line
DVD	Digital Video Disk

1.2.5 E

Acronym	Term
e-Commerce	Electronic Commerce
EDC	Enterprise Data Center
EDI	Electronic Data Interchange
EDP	Electronic Data Processing
EF	Exposure Factor
EIDE	Enhanced Integrated Drive Electronics

Acronym	Term
E-mail	Electronic Mail
EMI	Electromagnetic Interference
EO	Executive Order
EPHI (or ePHI)	Electronic Protected Health Information

1.2.6 F

Acronym	Term
FAR	Federal Acquisition Regulation
FBI	Federal Bureau of Investigation
FEA	Federal Enterprise Architecture
FIPS	Federal Information Processing Standards
FISCAM	Federal Information System Controls Audit Manual
FISMA	Federal Information Security Management Act
FMIB	Financial Management Investment Board
FPO	Fleet Post Office
FTI	Federal Tax Information (or Federal tax return information)
FS	Federal Standard
FTP	File Transfer Protocol

1.2.7 G

Acronym	Term
GAO	Government Accountability Office (formerly General Accounting Office)
GISRA	Government Information Security Reform Act
GOP	Grand Old Party
GSA	General Services Administration
GSS	General Support System
GTL	Government Task Lead

1.2.8 H

Acronym	Term
HCFA	Health Care Finance Administration
HIPAA	Health Insurance Portability and Accountability Act
HISM	Handbook of Information Security Management
HITR	HCFA Information Technology Reference
HMAC	Hash-based Message Authentication Code
HTTP	Hypertext Transfer Protocol

1.2.9 I

Acronym	Term
IA	Information Assurance
IBM	International Business Machines Corporation
ID	Identification
IDE	Integrated Drive Electronics
IDPS	Intrusion Detection and Prevention System
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronic Engineers
IKE	Internet Key Exchange
IMAP	Internet Message Access Protocol
INFOSEC	Information Security
IP	Internet Protocol
IPL	Initial Program Load
IPsec	Internet Protocol Security
IRC	Internal Revenue Code
IRS	Internal Revenue Service
IRSAP	Internal Revenue Service Acquisition Procedure
IS	Information System
ISA	Interconnection Security Agreement, or Information Security Agreement
ISO	International Organization for Standardization
ISS	Information Systems Security
ISSO	Information System Security Officer
ISSP	Information Systems Security Plan
ISSPH	Information Systems Security Plan Handbook
IT	Information Technology
ITA	Information Technology Architecture
ITMRA	Information Technology Management Reform Act
ITU	International Telecommunication Union
IV&V	Independent Validation &Verification

1.2.10 K

Acronym	Term
KDC	Key Distribution Center

1.2.11 L

Acronym	Term
LAN	Local Area Network
LBI	Limited Background Investigation

1.2.12 M

Acronym	Term
MA	Major Application
MAC	Medicare Administrative Contractor, or Message Authentication Code, or Mandatory Access Control
MBI	Minimum Background Investigation
MCM	Medicare Carriers Manual
MCS	Multiple Console Support
MDCN	Medicare Data Communications Network
MGT	Management
MitM	Man-in-the-Middle
MIM	Medicare Intermediary Manual
MIS	Management Information Services
MIT	Massachusetts Institute of Technology
MMA	Medicare Prescription Drug, Improvement, and Modernization Act
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MTD	Maximum Tolerable Downtime
MVS	Multiple Virtual Storage

1.2.13 N

Acronym	Term
NAC	National Agency Check
NACI	National Agency Check and Inquiries
NACIC	National Agency Check and Inquiries and Credit Check
NARA	National Archives and Records Administration
NASA	National Aeronautical and Space Administration
NC	Network Computer
NCSC	National Computer Security Center
NFS	Network File System
NIE	Net Impact Estimate
NIPC	National Infrastructure Protection Center

Acronym	Term
NIST	National Institute of Standards and Technology
NISTIR	National Institute of Standards and Technology Interagency Report
NOS	Network Operating System
NSA	National Security Agency
NSC	National Security Council
NSTISSIC	National Security Telecommunications and Information Systems Security Committee
NT	New Technology

1.2.14 O

Acronym	Term
OCSP	On-line Certificate Status Protocol
OIG	Office of Inspector General
OIS	Office of Information Services
OMB	Office of Management and Budget
OPM	Office of Personnel Management
OS	Operating System
OSI	Open Systems Interconnection
OTC	On-Time-Cost

1.2.15 P

Acronym	Term
P&P or Pol./Proc.	Policies and Procedures
P3P	Platform for Privacy Preferences Project
PC	Personal Computer
PDA	Personal Digital Assistants
PDF	Portable Document Format
PDS	Partitioned Data Sets
PHI	Protected Health Information
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIN	Personal Identification Number
PISP	Policy for the Information Security Program
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
PM	Project (Program) Managers
PO	Project Officer, or Procurement Office

Acronym	Term
POA&M	Plan of Action and Milestones
POL	Policy
POP	Post Office Protocol
PRCP	Project Review and Coordination Panel
PSGH	CMS Policy Standards and Guidelines Handbook
PSO	Physical Security Officer
PSSH	Personnel Security/Suitability Handbook
PUB	Publication

1.2.16 R

Acronym	Term
RA	Risk Assessment
RACF	Resource Access Control Facility
RAID	Redundant Array of Independent Disks
RAM	Random Access Memory
RDS	Remote Data Services
RFC	Request for Comments
RFI	Radio Frequency Interference
RFP	Requests for Proposals
RO	Regional Office
ROB	Rules of Behavior
ROE	Rules of Engagement
ROM	Regional Office Manual, or Read Only Memory
RPC	Remote Procedure Call
RPO	Recovery Point Objective
RTO	Recovery Time Objective

1.2.17 S

Acronym	Term
SA	Security Administrator
SAML	Security Assertion Markup Language
SAR	Safeguard Activity Report
SBI	Single Scope Background Investigation
SBU	Sensitive But Unclassified
SCA	Security Controls Assessment
SCSI	Small Computer System Interface

Acronym	Term
SDLC	System Development Life Cycle
SER	Scientific, Engineering, and Research
SII	Security/Suitability Investigations Index
SIRT	Security Incident Response Team
SISSO	Senior Information Systems Security Officer
SLE	Single Loss Expectancy
SM	System Manager
SMF	System Management Facility
S-MIME	Secure Multi-purpose Internet Mail Extensions
SMTP	Simple Mail Transfer Protocol
SOR	System of Records
SOW	Statement of Work
SP	Special Publication
SPR	Safeguard Procedures Report
SSA	System Security Administrator, or Social Security Administration
SSC	Systems Security Coordinator
SSH	Secure Shell
SSI	Security/Suitability Investigation
SSL	Secure Sockets Layer
SSM	Standard System Maintainers
SSN	Social Security Number
SSO	System Security Officer
SSP	System Security Plan
SSPM	System Security Plans Methodology
SSPS&G	System Security Policy Standards and Guidelines
SSPS&GH	System Security Policy Standards and Guidelines Handbook
SSSA	Senior Systems Security Advisor
SwA	Software Assurance
ST&E	Security Test and Evaluation (Obsolete [per 800-37 R1], See SCA)

1.2.18 T

Acronym	Term
TCP	Transmission Control Protocol
TDEA	Triple Data Encryption Algorithm
TG	Technical Guideline
TLS	Transport Layer Security
TMG	Technology Management Group

Acronym	Term
TO	Training Office

1.2.19 U

Acronym	Term
UID	User Identification (see also UserID)
UL	Underwriter's Laboratory
US-CERT	United States Computer Emergency Readiness Team
USB	Universal Serial Bus
USC (or U.S.C.)	United States Code
UserID (or USERID)	User Identification (see also UID)

1.2.20 V

Acronym	Term
VPN	Virtual Private Network

1.2.21 W

Acronym	Term
WAN	Wide Area Network
WAP	Wireless Application Protocol
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
WST	Web Support Team

1.2.22 X

Acronym	Term
XML	Extensible Markup Language

1.2.23 Y

Acronym	Term
Y2K	Year 2000

2 SOURCE REFERENCES

The terms and definitions in this document were obtained from multiple information assurance (IA) and information security sources including applicable laws, Executive Orders, directives, regulations, standards, policies, procedures, and guidelines. Except for international and institute standards (i.e., ISO, IEC, IEEE), and computer publications (i.e., Microsoft Press) which are not in the public domain, the other term and definition sources can be found at the following web sites:

- CMS: CMS IS policies, procedures, standards, and guidelines are available at the CMS IS "Virtual Handbook" web site: http://www.cms.hhs.gov/InformationSecurity/
- CNSSI: *National Information Assurance (IA) Glossary*, CNSSI 4009, June 2006, is available at: http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf
- DHHS: *Glossary of Key Enterprise Terms* is available at: http://www.hhs.gov/ocio/about/terms/index.html
- DHHS: *HHS Personnel Security/Suitability Handbook*, SDD/ASMB 1/98, is available at: http://www.hhs.gov/ohr/manual/pssh.pdf
- DHHS: DHHS security policies and standards are available at: http://www.hhs.gov/ocio/policy/#Security
- Executive Orders: http://www.archives.gov/federal-register/executive-orders/disposition.html
- GAO: *Federal Information System Controls Audit Manual (FISCAM),* GAO-09-232G, February 2, 2009, is available at: http://www.gao.gov/new.items/d09232g.pdf
- Homeland Security Presidential Directives: http://www.dhs.gov/xabout/laws/editorial_0607.shtm
- IRS: Publication 1075 can be found at: http://www.irs.gov/pub/irs-pdf/p1075.pdf
- NIST: FIPS Publications are available at: http://csrc.nist.gov/publications/PubsFIPS.html
- NIST: NISTIRs are available at: http://csrc.nist.gov/publications/PubsNISTIRs.html
- NIST: *Glossary of Key Information Security Terms*, NIST IR 7298, Revision 1,February 2011, at: http://csrc.nist.gov/publications/nistir/ir7298-rev1/nistir-7298-revision1.pdf
- NIST: SP 800- series documents are available at: http://csrc.nist.gov/publications/PubsSPs.html
- OMB: OMB Circulars can be found at the CMS IS "Virtual Handbook" web site or at: http://www.whitehouse.gov/omb/circulars/index.html
- OMB: OMB Memoranda can be found at the CMS IS "Virtual Handbook" web site or at: http://www.whitehouse.gov/omb/memoranda_default/
- US-CERT: *IT Security Essential Body of Knowledge (EBK): A Competency and Functional Framework for IT Workforce Development* can be found at:

  http://www.us-cert.gov/ITSecurityEBK/
- *Telecommunications: Glossary of Telecommunication Terms*, Federal Standard 1037C, August 7, 1996, can be found at: http://www.its.bldrdoc.gov/fs-1037/fs-1037c.htm

- The Internet Engineering Task Force (IETF) RFCs can be retrieved at: http://www.ietf.org/rfc.html
- Wikipedia can be found at: http://en.wikipedia.org/wiki/Main_Page

The CMS IS "Virtual Handbook" web site provides a list of applicable laws across the program. Some additional references are provided below:

- Public Law 74-271, *Social Security Act*, as amended http://www.ssa.gov/OP_Home/ssact/ssact.htm.htm
- Public Law 93-579, *The Privacy Act of 1974*, as amended http://www.usdoj.gov/foia/privstat.htm
- Public Law 104-13, *Paperwork Reduction Act of 1995* http://www.gpo.gov/fdsys/pkg/PLAW-104publ13/pdf/PLAW-104publ13.pdf
- Public Law 107-347, *E-Government Act of 2002*, as amended http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf
- Public Law 108–173, *Medicare Prescription Drug, Improvement, and Modernization Act of 2003 (MMA*), SEC. 912: Requirements for Information Security for Medicare Administrative Contractors http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_public_laws&docid=f:publ173.108.pdf
- *Code of Federal Regulations (CFR)*, Regulation 5 CFR Part 731 – Suitability, 5CFR731 http://www.access.gpo.gov/nara/cfr/waisidx/5cfr731.html
- United States Code Title 44 Chapter 33—*Disposal of Records* http://www.archives.gov/about/laws/disposal-of-records.html
- United States Code Title 44 Chapter 35—*Coordination of Federal Information Policy* http://www.gpo.gov/fdsys/pkg/USCODE-2010-title44/pdf/USCODE-2010-title44-chap35.pdf

3 APPROVED

teresa.fryer@cms.hhs.gov

Digitally signed by teresa.fryer@cms.hhs.gov
DN: cn=teresa.fryer@cms.hhs.gov
Date: 2012.07.16 13:27:20 -04'00'

Teresa Fryer
CMS Chief Information Security Officer and
Director, Enterprise Information Security Group

This document will be reviewed periodically, but no less than annually, by the Enterprise Information Security Group (EISG), and updated as necessary to reflect changes in policy or process. If you have any questions regarding the accuracy, completeness, or content of this document, please contact the EISG at mailto:ciso@cms.gov.

(This Page Intentionally Blank)