DEPARTMENT OF HEALTH & HUMAN SERVICES
Centers for Medicare & Medicaid Services
7500 Security Boulevard, Mail Stop N2-14-26
Baltimore, Maryland 21244-1850

CENTERS FOR MEDICARE & MEDICAID SERVICES (CMS)
Office of Information Services (OIS)
Security and Standards Group (SSG)
7500 Security Blvd
Baltimore, MD 21244-1850

CMS Information Security Terms & Definitions

Version 3.0
October 7, 2005

Summary of changes in the CMS Information Security Terms and Definitions v3.0

1) Eliminated duplicate Password definitions (password and passwords).
2) Added definition narrative to Warning Banner.
3) Includes the following additions to terms and definitions as a result of the *CMS Information Security Approach, Acceptable Risks Safeguards, version 2.0; and CMS e-Authentication Standards*:

Listed additions

e-Authentication,
Address of Record,
Attack,
Attacker,
Approved,
Assertion,
Asymmetric Keys,
Authentication,
Authentication Protocol,
Authenticity,
Bit,
Biometric,
Certification Authority (CA),
Certificate Revocation List (CRL),
Challenge-Response Protocol,
Claimant,
Credential,
Credentials Service Provider (CSP),
Cryptographic Key,
Cryptographic Strength,
Cryptographic YToken,
Data Integrity,
Digital Signature,
Electronic Credentials,
Entropy,
FIPS,
Guessing Entropy,
Hash Function,
HMAC,
Identity,
Identity Proofing,
Kerberos,
Man-in-the-Middle Attack (MitM),
Message Authentication Code (MAC),
Min-Entropy,
Network
Nonce,
Off-line Attack,
On-line Attack,
On-Line Certificate Status Protocol (OCSP),
Passive Attack,
Password,
Possession and Control of a Token,
Personal Identification Number (PIN),
Practice Statement,
Private Key,
Proof of Possession (PoP) Protocol,
Protocol Run,
Public Key,
Public Key Certificate,
Pseudonym,
Registration,
Registration Authority (RA),
Relying Party,
Salt,
Security Assertion Markup Language (SAML),
Shared Secret,
Subject,
Subscriber,
Symmetric Key,
Token,
Transport Layer Security (TLS),
Tunneled Password Protocol,
Verified Name,
Verifier,
Zero Knowledge Password; and
Zero Knowledge Protocol.

GLOSSARY

1. INTRODUCTION

The CMS Information Security Terms and Definition resource tool provides definitions for common terms in information security. Terms are listed in alphabetical order together with the definition that applies within the CMS Information Security Program. Due to contractual issues, some terms have different definitions that only apply to the CMS Fiscal Intermediaries and Carriers. In these instances, the applicable definition is preceded by "**(BPSSM)"** which means Business Partners Systems Security Manual.

2. TERMS AND DEFINITIONS

The tables for terms and definitions begin on the next page.

TERMS	DEFINITIONS
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.
ACCESS	The ability or the means necessary to "read", "write", modify or communicate data or otherwise make use of any system resource. **(BPSSM)** A specific type of interaction between a subject and an object that results in the flow of information from one to the other. (National Computer Security Center(NCSC)-TG-004) Opportunity to make use of an information system (IS) resource. National Security Telecommunications and Information Systems Security Committee (NSTISSI)
ACCESS CONTROL	The means of limiting access to information or to resources of a computer system to authorized users. **(BPSSM)** Controls designed to protect computer resources from unauthorized modification, loss, or disclosure. Access controls include both physical access controls, which limit access to facilities and associated hardware, and logical controls, which prevent or detect unauthorized access to sensitive data and programs that are stored or transmitted electronically. Federal Information System Controls Audit Manual (FISCAM).
ACCESS CONTROL LIST (ACL)	A list of entities that are authorized to have access to a resource, together with their access methods.
ACCESS CONTROL SOFTWARE	Mechanisms that restrict access to computer resources. E.g. RACF, TOP SECRET. **(BPSSM)** This type of software (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 generally can 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 warning, 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)
ACCESS PATH	The path through which user requests travel, including the telecommunications software, transaction processing software, application program, etc. (FISCAM) 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.
ACCESS SCRIPT	A program or a series of encoded commands that enable a user to log-on to a system.

TERMS	DEFINITIONS
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.
ACCOUNTABILITY **See "Non-Repudiation"**	The repercussions of actions taken by individuals. **(BPSSM)** The existence of a record that permits the identification of an individual who performed some specific activity so that responsibility for that activity can be established. (FISCAM)
ACCREDITATION	The official management authorization for the operation of an application and is based on the certification process and other management considerations. Automated Information Systems Security Program (AISSP) Federal Information Processing Standards (FIPS PUB 102) A formal declaration by the Designated Approving Authority (DAA) that the AIS is approved to operate in a particular security mode using a prescribed set of safeguards. Accreditation is the official management authorization for operation of AIS and is based on the certification process as well as other management considerations. The accreditation statement assigns security responsibilities to the DAA and shows that due care has been taken for security. (NCSC-TG-004)
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 box number, Fleet Post Office 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.
AGENCY	Agency means any executive department, military department, Government corporation, Government-controlled corporation, or other establishment in the executive branch of the Government, or any independent regulatory agency. Within the Executive Office of the President, the term includes only the Office of Management and Budget (OMB) and Office of Administration. (OMB Circular A-130)
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 s/he 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.
ANTI-VIRUS 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.

TERMS	DEFINITIONS
APPLICATION	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. **(BPSSM)** A computer program designed to help people perform a certain type of work, including specific functions, such as payroll, inventory control, accounting, and mission support. Depending on the work for which it was designed, an application can manipulate text, numbers, graphics, or a combination of these elements.
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 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 PROGRAMS	See Application
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 which is written to perform a specific business function (may include some Commercial Off-\The-Shelf (COTS) software)
APPLICATION SYSTEM MANAGER	See Application Manager
APPLICATION SYSTEMS	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. (AISSP) (FIPS PUB 11-3)
APPROVED	FIPS-approved or NIST recommended. An algorithm or technique that is either: 1) Specified in a FIPS or NIST Recommendation; or 2) Adopted in a FIPS or NIST Recommendation. Approved cryptographic algorithms must be implemented in a crypto-module validated under FIPS 140-2. For more information on validation and a list of validated FIPS 140-2 validated crypto-modules see http://csrc.nist.gov/cryptval/.

TERMS	DEFINITIONS
ARCHITECTURE	A design. The term architecture can refer to either hardware or software, or to a combination of hardware and software. The architecture of a system always defines its broad outlines, and may define precise mechanisms as well for e.g., it may describe functional requirements of the system and the information interaction between entities of the system.
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.
ASSET	All objects contained within an organization, both physical (e.g. buildings, personal hardware) and logical (e.g. data, services). **(BPSSM)** Any software, data, hardware, administrative, physical communications, or personnel resource within an Automatic Data Processing (ADP) system of activity.
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	All activities taken to demonstrate the conformity of a product to pre-specified criteria.
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.
ATTACK	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) **Acceptable Risk Safeguards (ARS)** An attempt to obtain a subscriber's token or to fool a verifier into believing that an unauthorized individual possesses a claimant's token. (ARS draft v2.0)
ATTACKER	Party who is not the claimant or verifier but who wishes to execute the authentication protocol successfully as a claimant.

TERMS	DEFINITIONS
AUDIT	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). **(BPSSM)** 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. (NSTISSI)
AUDIT TRAIL	A record showing who has accessed a computer system and what operations s/he 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. **(BPSSM)** In an accounting package, any program feature that automatically keeps a record of transactions to support backtracking to find the origin of specific figures that appears on reports. In computer systems, a step-by-step history of a transaction, especially a transaction with security sensitivity. Includes source documents, electronic logs, and records of accesses to restricted files. (FISCAM)
AUTHENTICATION	The act of verifying a claimed identity of individual, station or originator. **(BPSSM)** The act of verifying the identity of a user and the user's eligibility to access computerized information. Designed to protect against fraudulent activity. (FISCAM) **(ARS)**The process of establishing confidence in user identities. (ARS draftv2.0)
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 cryptographically.
AUTHENTICITY	The quality of data integrity that originates from its purported source.
AUTHORIZATION	The acceptance that a requestor has permission to access a resource.
AUTOMATED INFORMATION SYSTEM (AIS)	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. **(BPSSM)** The organized collection, processing, transmission, and dissemination of automated information in accordance with defined procedures. (AISSP) (OMB Circular A-130)
AUTOMATED INFORMATION SECURITY	See Systems Security

TERMS	DEFINITIONS
AVAILABILITY	The assurance that authorized users have access to information and assets when required.
BACK OFFICE FUNCTION	An office, building, or function that is used by an organization to conduct support activities.
BACKUP	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. **(BPSSM)** 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 Plans
BASIC INPUT OUTPUT SYSTEM (BIOS)	The program that starts up your computer and communicates between the devices in your computer (such as your hard drive and graphics card) and the system.
BASELINE	An agreed upon specification or standard against which changes can be made. A baseline should be changed only through formal change control procedures.
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)
BIOMETRIC	An image or template of a physiological attribute (e.g., a fingerprint) that may be used to identify an individual. In this document, biometrics may be used to unlock authentication tokens and prevent repudiation of registration.
BIOMETRIC AUTHENTICATION	The verification of an individual identity on the basis of a unique and measurable physical characteristic, such as a fingerprint. **(BPSSM)** 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)
BIT	A binary digit: 0 or 1.

TERMS	DEFINITIONS
BREACHES	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. **(BPSSM)** The successful and repeatable defeat of security controls with or without an arrest, which if carried to consummation, could result in a penetration of the system. Examples of breaches are: -Operation of user code in master mode. -Unauthorized acquisition of identification password or file access passwords. -Accessing a file without using prescribed operating system mechanisms. -Unauthorized access to tape library.
BROWSING	The act of electronically perusing files and records without authorization. (FISCAM) 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. (NCSC-TG-004)
BUFFER OVERFLOW	The act of introducing arbitrary code executed on a system which does not adequately check input for appropriate length.
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 & 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 emergency situations.
BUSINESS IMPACT ANALYSIS (BIA)	The process of analyzing current and planned business functions and the effect that their interruption in service may have on the organization.

TERMS	DEFINITIONS
BUSINESS OWNER / PARTNER	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. **(BPSSM)** 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. CMS business partners are Standard Systems Maintainers (SSM), Common Working File (CWF) host sites, Durable Medical Equipment Regional Carrier (DMERC), Data Centers and other specialty contractors.
CERTIFICATE	Security information signed electronically by an authority and used as identification. Certificates are generally signed using public key technology.
CERTIFICATE REVOCATION LIST (CRL)	A list of revoked public key certificates created and signed digitally by a Certification Authority. See [RFC 3280]
CERTIFICATION	Certification consists of a technical evaluation of a sensitive application to see how well it meets security requirements. (FIPS PUB 102) **(BPSSM)** Consists of a technical evaluation of a sensitive application to see how well it meets security requirements. (AISSP) (FIPS PUB 102) A formal process by which an agency official verifies, initially or by periodic reassessment, that a system's security features meet a set of specified requirements.
CERTIFICATION AUTHORITY (CA)	A trusted entity that issues and revokes public key certificates.
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.

TERMS	DEFINITIONS
CHECK POINT	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)
CHIEF INFORMATION OFFICER (CIO)	The **CIO** is responsible for the implementation and administration of the AIS Security Program within an organization.
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. **(BPSSM)** Information that has been determined pursuant to Executive Order 12958 or any predecessor Order, or by the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure and is marked to indicate its classified status. (NSTISSI)
CODE	Instructions written in a computer programming language. (See object code and source code.) (FISCAM)
COLD SITE	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. **(BPSSM)** An IS 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 computer equipment in the event that the user has to move from their main computing location to an alternative computing location. (FISCAM)
COMMANDS	A job control statement or a message, sent to the computer system, that initiates a processing task. (FISCAM)
COMMERCIAL OFF THE SHELF (COTS)	Proprietary hardware or software produced in quantity and purchased from business suppliers to meet an organizational need.
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. **(BPSSM)** Measures and controls taken to deny unauthorized persons information derived from telecommunications and to ensure the authenticity of such telecommunications. Communications security includes crypto-security, transmission security, emission security, and physical security of COMSEC material. (NSTISSI)
COMPACT DISC-READ ONLY MEMORY (CD-ROM)	A form of optical rather than magnetic storage. CD-ROM devices are generally “read-only”. (FISCAM)

TERMS	DEFINITIONS
COMPATIBILITY	The ability of two or more systems or components seamlessly to perform required services. **(BPSSM)** 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	An internal control that reduces the risk of an existing or potential control weakness that could result in errors or omissions (FISCAM)
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	An unauthorized disclosure or loss of sensitive defense data. (FIPS PUB 39)
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 NETWORK	See Network.
COMPUTER OPERATIONS	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
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 Systems Security and Systems Security.
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.] (AISSP) (Source: NIST SPEC PUB 800-3)

TERMS	DEFINITIONS
COMPUTER SYSTEM	A complete computer installation, including peripherals, in which all the components are designed to work with each other. (FISCAM) 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. (AISSP) (Computer Security Act of 1987)
CONFIDENTIALITY	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. **(BPSSM)** Ensuring that transmitted or stored data are not read by unauthorized persons. (FISCAM)
CONFIGURATION	The arrangement or setup of a computer system, application or component based upon system environment and organizational requirements.
CONFIGURATION MANAGEMENT (CM)	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 **(BPSSM)** 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	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. **(BPSSM)** 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.

TERMS	DEFINITIONS
CONTINGENCY PLAN (CP)	A Contingency Plan is a plan for emergency response, backup procedures, and post disaster recovery. Synonymous with Disaster Plan and Emergency Plan. See Business Continuity & Contingency Plan **(BPSSM)** 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 failure, or disaster. (FISCAM) A plan for emergency response, backup procedures, and post-disaster recovery. Synonymous with Disaster Plan and Emergency Plan. (AISSP) (FIPS PUB 11-3)
CONTINGENCY PLANNING	The process for ensuring, in advance, that any reasonable and foreseeable disruptions will have a minimal effect. (ISSPH - Glossary) See Contingency Plan. (FISCAM)
CONTINUITY OF OPERATIONS PLAN (COOP)	See Business Continuity & Contingency Plan
CONTRACTORS	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. (Appendix A.)
COST DETERMINATION	The value of efforts determined necessary to moderate identified risks. Cost factors may include labor, time, system response, and financial considerations.
COUNTERMEASURES	Actions and system controls present or undertaken to reduce or moderate the effect of specific vulnerabilities.
CREDENTIAL	An object that authoritatively binds an identity (and optionally, additional attributes) to a token possessed and controlled by a person.
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.
CRISIS	A critical event that has the ability to impact 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.
CRITICALITY	The level of impact an interruption in service or exposure will have on an organization.

TERMS	DEFINITIONS
CRYPTOGRAPHIC KEY	A value used to control cryptographic operations, such as decryption, encryption, signature generation or signature verification. For the purposes of this document, keys must provide at least 80-bits of protection. This means that it must be as hard to find an unknown key or decrypt a message, given the information exposed to an eavesdropper by an authentication, as to guess an 80-bit random number. See also Asymmetric keys, Symmetric key.
CRYPTOGRAPHIC STRENGTH	A measure of the expected number of operations required to defeat a cryptographic mechanism. For the purposes of this document, this term is defined as meaning that breaking or reversing an operation is at least as difficult computationally as finding the key of an 80-bit block cipher by key exhaustion (it requires at least on the order of 279 operations).
CRYPTOGRAPHIC TOKEN	A token where the secret is a cryptographic key.
CRYPTOGRAPHY	The principles, means, and methods for rendering information unintelligible and for restoring encrypted information to intelligible form for an authorized party. **(BPSSM)** The science of coding messages so they cannot be read by any person other than the intended recipient. Ordinary text or plain text and other data are transformed into coded form by encryption and translated back to plain text or data by decryption. (FISCAM)
DAMAGE ASSESSMENT	Post-incident appraisal or determination of actual consequences to an organization including human, physical, economic, reputation and natural resource impacts.
DATA	A representation of facts, concepts or instructions in a manner suitable for communication, interpretation or processing by human or electronic means. **(BPSSM)** Facts and information that can be communicated and manipulated. (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	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) The transfer of data between functional units by means of data transmission according to a protocol. (AISSP) (FIPS PUB 11-3)
DATA CONTAMINATION	The introduction of data of one sensitivity level into data of a lower or different sensitivity level. An accidental or intentional violation of data integrity.

TERMS	DEFINITIONS
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	A data dictionary 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 for each data element in the organization's files and databases. **(BPSSM)** 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 ENCRYPTION STANDARDS (DES)	The conversion of data into an unintelligible form so that it is readable except by authorized users is called data encryption. The DES is an approved FIPS cryptographic algorithm which is as required by FIPS 140-1 **(BPSSM)** A NIST Federal Information Processing Standard and a commonly used secret-key cryptographic algorithm for encrypting and decrypting data. (FISCAM) The National Institute of Standards and Technology **Data Encryption Standard** was adopted by the U.S. Government as Federal Information Processing Standard (FIPS) Publication 46 [at publication 46-1], which allows only hardware implementations of the data encryption algorithm. (AISSP) (FIPS PUB 11-3)
DATA FILE	See File.
DATA INTEGRITY	The assurance that computerized data has not been exposed to accidental or malicious modification, alteration, or destruction. **(ARS)** The property that data has not been altered by an unauthorized entity. (ARS draft v2.0)
DATA OWNERS	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	The process whereby a computer and its programs organize / manipulate data and the flow of data. **(BPSSM)** 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 PUB 39) See Security Management Function.

TERMS	DEFINITIONS
DATA VALIDATION	Checking transaction data for any errors or omissions that can be detected by examining the data. (FISCAM)
DATA BASE	A system of organized files of related data. **(BPSSM)** 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)
DATABASE MANAGEMENT SYSTEM (DBMS)	Database Management Systems are a set of programs that control the organization, storage and retrieval of data. The database management system also controls the security and data integrity of the database. **(BPSSM)** 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	Degauss is to demagnetize a monitor or the read/write head in a disk or tape drive to neutralize unwanted magnetism or remove unwanted data. To remove a residual magnetic field from a magnetized object, usually by introducing much stronger and gradually diminishing magnetic fields of alternating polarity. Specifically, to erase information from a magnetic storage medium by degaussing. **(BPSSM)** To apply a variable, alternating current (AC) field for the purpose of demagnetizing magnetic recording media. The process involved increases the AC field gradually from zero to some maximum value and back to zero, which leaves a very low residue of magnetic induction on the media. (FIPS PUB 39)
DEMILITARIZED ZONE (DMZ)	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.

TERMS	DEFINITIONS
DENIAL-OF-SERVICE (DOS)	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. **(BPSSM)** Any action or series of actions that prevent any part of a system from functioning in accordance with its intended purpose. This includes any action that causes unauthorized destruction, modification, or delay of service. Synonymous with interdiction. (NCSC-TG-004)
DIAL-UP ACCESS	A method of accessing a computer system remotely using telephone lines and a modem. **(BPSSM)** A means of connecting to another computer or a network like the Internet, over a telecommunications line using a modem-equipped computer. (FISCAM)
DIGITAL SIGNATURE	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. **(ARS)** An asymmetric key operation where the private key is used digitally to sign an electronic document and the public key is used to verify the signature. Digital signatures provide authentication and integrity protection. (ARS draft v2.0)
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)	The document or documents defining the resources, actions, tasks, and data required for restoring the business processes in the event of an interruption. **(BPSSM)** A written plan for processing critical applications in the event of a major hardware or software failure or destruction of facilities. (FISCAM)
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.
DISCRETIONERY ACCESS CONTROL	Controls that regulate how users delegate access permissions or make files / information accessible to other users.
DISKETTE	A removable and widely used data storage medium that uses a magnetically coated flexible disk of Mylar enclosed in a plastic case. (FISCAM)

TERMS	DEFINITIONS
DOMAIN	The scope of operations for an application or system.
E-AUTHENTICATION	The process of establishing reasonable confidence in user identities presented electronically to an information system in order to conduct transactions.
EAVESDROPPING	The action of unobserved listening to conversations between people or systems in order to obtain information.
ELECTRONIC CREDENTIALS	Digital documents used in authentication that bind an identity or an attribute to a subscriber's token. Note that this document distinguishes between credentials, and tokens (see below) while other documents may interchange these terms.
ELECTRONIC MAIL (E-MAIL)	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. An e-mail system requires a messaging system, which provides the "store" and "forward" capability, and an e-mail program that provides the user interface with "send" and "receive" functions. The Internet revolutionized e-mail by turning countless incompatible islands into one global system. The Internet initially served its own members, of course, but then began to act as an e-mail gateway between the major on-line services. It then became *the* messaging system for the planet. (Technical Encyclopedia (TechEncy))
ELECTRONIC SIGNATURE	A symbol, generated by electronic means, that can be used to (1) identify the sender of information and (2) 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 (1) unique to the signer, (2) under the signer's sole control, (3) capable of being verified, and (4) 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)
EMERGENCY CO-ORDINATOR	The system member responsible for assessing emergency situations and making decisions to respond.
ENCRYPTION	The transformation of plain text (words) into cipher text (unintelligible) by cryptographic techniques in order to protect data from disclosure during network transmissions. **(BPSSM)** The transformation of data into a form readable only by using the appropriate key held only by authorized parties. (FISCAM)
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.

TERMS	DEFINITIONS
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	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.
ENVIRONMENT CONTROLS	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 OS Software) and software and utility programs that are used in the development of applications and/or databases (e.g. DB2, Oracle DB, Cobol, M204 and GSS COTS software). (SSP Methodology)
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.
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 which provides the ability to initiate a program. (FISCAM)
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.
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. **(BPSSM)** See Computer Facility
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 records stored in computerized form. (FISCAM)
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 PERMISSIONS	Access attributes associated with a file or directory, as defined in an 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.
FIPS	Federal Information Processing Standard.

TERMS	DEFINITIONS
FIREWALL	Software and/or hardware deployed to maintain control over information going into and out of a network. 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. **(BPSSM)** 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)
FRAUD	A deception deliberately practiced to secure unfair or unlawful gain.
GATEWAY	In a communications network, a network node equipped to interface with another network that uses different protocols. (BPSSM) In networks, a computer that connects two dissimilar local area networks, or connects a LAN to a wide area network, minicomputer, or mainframe. A gateway may perform network protocol conversion and bandwidth conversion. (FISCAM)
GENERAL CONTROLS	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)

TERMS	DEFINITIONS
GENERAL SUPPORT SYSTEMS (GSS)	Computer platform that incorporates hardware, operating system software, and environmental software to support major applications, e.g. data center, web hosting, web services – Medicare Data Communications Network (MDCN). 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. (System Security Plan (SSP) Methodology) **(BPSSM)** An interconnected set of information resources under the same direct management control that shares common functionality. Normally, the purpose of a General Support System (GSS) is to provide processing or communication support. (FISCAM) 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 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. (SSPS&GH - Glossary)(Source: OMB Circular A-130)
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	Those media in which a message flows through a physical media (e.g., twisted pair wire, coaxial cable). Provides a closed path between sender and receiver over Twisted Pair (e.g. Telephone cable), Coaxial Cable, and Optical Fiber. (Computer Assisted Technology Transfer Laboratory, Oklahoma State University)
GUIDELINES	Recommended security configurations, policies or actions developed to provide assistance in complying with one or more policies or standards.
HACKER	An outside individual who attempts to access and/or compromise the confidentiality, integrity or availability of organizational data or systems.

TERMS	DEFINITIONS
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 ADP system or communicated, displayed, produced, or disseminated by an ADP system.
HARDWARE	The physical part of a computer system including the machinery and equipment. **(BPSSM)** 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: 1. (One-way) It is computationally infeasible to find any input which maps to any pre-specified output, and 2. (Collision resistant) It is computationally infeasible to find any two distinct inputs that map to the same output.
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.
HMAC	Hash-based Message Authentication Code: a symmetric key authentication method using hash functions.
HOTSITE	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).
IDENTIFICATION (ID)	The process that enables recognition and validation of an entity by a system.
IDENTITY	A unique name of an individual person. Since the legal names of persons are not necessarily unique, the identity of a person must include sufficient additional information (for example an address, or some unique identifier such as an employee or account number) to make the complete name unique.
IDENTITY PROOFING	The process by which a Customer Service Plan (CSP) and a RA validate sufficient, unique information to identify a person.
IMAGE	An exact copy of what is on the storage medium.
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)

TERMS	DEFINITIONS
INCIDENT	Any adverse event whereby some aspect of computer security could be threatened: loss of data confidentiality, disruption of data or system integrity, or disruption or Denial-of-Service. **(BPSSM)** A computer security incident is any adverse event whereby some aspect of computer security could be threatened: loss of data confidentiality, disruption of data or system integrity, or disruption or Denial-of-Service**.**
INCIDENT RESPONSE PROCEDURE	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. (*CMS Incident Response Procedure*) 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.
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 VERIFICATION & VALIDATION	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.
INFORMATION	Data in any form. **(BPSSM)** The meaning of data. Data are facts; they become information when they are seen in context and convey meaning to people. (FISCAM AISSP). 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. (AISSP) (OMB Circular A-130)
INFORMATION RESOURCE	See Resource.
INFORMATION RESOURCE OWNER	See Owner
INFORMATION SECURITY	The protection of data against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional to preserve the confidentiality, integrity and availability of the system.
INFORMATION SECURITY TRAINING AND AWARNESS	Training in organizational policies and procedures, security requirements, legal responsibilities, business controls, and correct, safe use of information processing facilities.
INFORMATION SYSTEMS (IS)	The entire infrastructure, organization, personnel, and components for the collection, processing, storage, transmission, display, dissemination, and disposition of information. (NSTISSI)

TERMS	DEFINITIONS
INFORMATION SYSTEMS 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.] (AISSP) (NISTIR 4659) (See also Systems Security)
INFORMATION SYSTEMS SECURITY OFFICER (ISSO)	Person responsible for ensuring the security of an information system throughout its life-cycle, from design through disposal. Synonymous with SSO. (NSTISSI)
INFORMATION TECHNOLOGY (IT)	Processing information by computer. (TechEncy) The definition varies from simple automation of manual processes using microprocessors to computers to networks to desktop publishing to networking. (Source: U. Texas)
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)
INTEGRITY	The assurance that information and programs are changed only in a specified and authorized manner. **(BPSSM)** 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)
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 CONTROL	A process, implemented by agency management and other personnel, designed to provide reasonable assurance that (1) operations, including the use of agency resources, are effective and efficient; (2) financial reporting, including reports on budget execution, financial statements, and other reports for internal and external use, are reliable; and (3) 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 (5) 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 CONNECTIVITY	A computer or network connection to an organizational peer system within the defined security perimeter.

TERMS	DEFINITIONS
INTERNET	Refers to the collection of networks and gateways that use the Transmission Control Protocol /Internet Protocol (TCP/IP) suite of protocols. (FISCAM)
INTRUSION	Unauthorized access to logical and physical resources.
INTRUSION DETECTION SYSTEMS (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.
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.
IPL	See Initial Program Load.
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)
JUNK MAIL (E-MAIL)	Transmitting e-mail to unsolicited recipients. U.S. federal law 47USC227 prohibits broadcasting junk faxes and e-mail, allowing recipients to sue the sender in Small Claims Court for $500 per copy. (TechEncy)
KERBEROS	A widely used authentication protocol developed at 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.
KERNEL FLAW	Any security flaw that occurs in the kernel code of an operating system.
KEY	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. **(BPSSM)** 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	Supervision and control of the process whereby a key is generated, stored, protected, transferred, loaded, used, and destroyed. (NSTISSI)
KEYSTROKE MONITORING	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 AIS returns to the user. **(BPSSM)** A process whereby computer system administrators view or record both the keystrokes entered by a computer user and the computer's response during a user-to-computer session. (AISSP – Source: *CSL Bulletin*)

TERMS	DEFINITIONS
LABEL	The marking of an item or information to reflect its information category and/or security classification.
LEAST PRIVILEGE	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.
LIBRARY	A program library is a collection of (usually) pre-compiled, reusable programming routines that a programmer can "call" when writing code. **(BPSSM)** 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 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 / LIFE-CYCLE MODEL	Spans the entire time that a project / program including hardware and software is being planned, designed, developed, procured, installed, used, and retired from service. 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. (Source: 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	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. (SSPS&GH - Glossary)
LOAD LIBRARY	A 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)

TERMS	DEFINITIONS
LOCAL AREA NETWORK (LAN)	An interconnected computing environment that enables data sharing at a single location. This type of network does not utilize a public carrier. 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. (SSP Methodology) **(BPSSM)** 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)
LOGS OR LOGGING FILE	A record of a computer's, network's or application's activity, used for system information, backup, and recovery. **(BPSSM)** With respect to computer systems, a record of an event or transaction. (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)
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	A technical means of controlling what information users can utilize, the programs they can run, and the modifications they can make. **(BPSSM)** 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)
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.
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. **(BPSSM)** Faking the sending address of a transmission in order to gain illegal entry into a secure system. (TechEncy)

TERMS	DEFINITIONS
MAINFRAME SYSTEMS	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	Periodic upkeep of computer systems including clearing of log files, installation of patches and system upgrades. **(BPSSM)** 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) The process of retaining a hardware system or component in, or restoring it to, a state in which it can perform its required functions. (Source: IEEE Std 610.12-1990)
MAJOR APPLICATION (MA)	A Major Application (MA) consists of data and customized application software only. It is housed on one or more GSSs. **(BPSSM)** OMB Circular A-130 defines an MA as an application that requires special attention due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information in that application. (FISCAM) 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. A breach in a major application might compromise many individual application programs, hardware, software, and telecommunications components. A MA can be either a major software application or a combination of hardware / software. Its sole purpose is to support a specific mission-related function. (Information Systems Security Plan Handbook (ISSPH) - Glossary)
	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 MAs. Adequate security for other applications should be provided by security of the systems in which they operate. (OMB Circular A-130) All "Major Applications" require "special management attention." The SSP for a MA may be defined broadly enough to include hardware, software, networks, and even facilities where it is reasonable. This permits the systems to have reasonable boundaries for the purposes of security planning.

TERMS	DEFINITIONS
MALICIOUS CODE	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. **(BPSSM)** The collective name for a class of programs intended to disrupt or harm systems and networks. The most widely known example of malicious software is the computer virus; other examples are Trojan horses and worms. (AISSP – Source: DHHS Definition, adapted from NIST SPEC PUB 500-166)
MANAGEMENT CONTROLS	Controls put in place to manage computer security systems or applications and the associated risks.
MAN-IN-THE-MIDDLE ATTACK (MITM)	An attack on the authentication protocol run in which the attacker positions himself in between the claimant and verifier so that he can intercept and alter data traveling between them.
MASTER CONSOLE	In MVS environments, the master console provides the principal means of communicating with the system. Other multiple console support (MCS) consoles often serve specialized functions, but can have master authority to enter all MVS commands. (FISCAM)
MASTER FILE	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. **(BPSSM)** 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 ADP system regardless of form or medium, e.g., programs, reports, data sets or files, records, and data elements.
MEDIA (Storage Media)	Physical objects such as paper, PC, and workstation diskettes, 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. (SSPS&GH)
MESSAGE AUTHENICATION CODE (MAC)	A cryptographic checksum on data that uses a symmetric key to detect both accidental and intentional modifications of the data.
METHODOLOGY	The logic applied to define a process. **(BPSSM)** The specific way of performing an operation that implies precise deliverables at the end of each stage. (TechEncy)

TERMS	DEFINITIONS
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 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 NACIC and can be used for selected public trust positions.
MISSION CRITICAL	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. **(BPSSM)** Vital to the operation of an organization. In the past, mission-critical information systems were implemented on mainframes and minicomputers. Increasingly, they are being designed for and installed on personal computer networks. (TechEncy)
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. (SSPS&GH - Glossary)
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)
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.
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 FBI Identification Division's name and fingerprint files, and other files or indices when necessary. (SSPS&GH - Glossary)
NEED-TO-KNOW	The necessity for access to, or knowledge or possession of, specific information required to carry out official duties. (NSTISSI)

TERMS	DEFINITIONS
NETWORK	A telecommunications medium which, with associated components, is a means of exchanging information. **(BPSSM)** 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. Small or large, a computer network exists to provide computer users with the means of communicating and transferring information electronically. (AISSP – Source: *Microsoft Press Computer Dictionary*) **(ARS)** 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 (claimant, verifier, CSP or relying party). (ARS draft v2.0)
NETWORK ARCHITECTURE	The description of an information-sharing environment.
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.
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.
NON-PRIVILEGED ACCESS	Cannot bypass any security controls.
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)

TERMS	DEFINITIONS
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.
OFFICE OF INFORMATION SYSTEMS (OIS)	CMS Office that ensures the effective management of CMS's information systems and resources. The office also develops and maintains central databases and statistical files, and directs Medicare claims payment systems.
ON-LINE	Available for immediate use. It typically refers to being connected to the Internet or other remote service. When connected via modem, a user is on-line after s/he dials-in and logs-on to his/her Internet provider with his/her username and password. When a user logs-off, s/he is off-line. With cable modem and DSL service, a user is on-line all the time. A peripheral device (terminal, printer, etc.) that is turned on and connected to the computer is also on-line. (TechEncy)
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].
OPERATING SYSTEM	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 operating system is to provide an environment in which a user can execute programs in a convenient and efficient manner. **(BPSSM)** The master control program that runs the computer. It is the first program loaded when the computer is turned on, and its main part, called the kernel, resides in memory at all times. It may be developed by the vendor of the computer in which it is running or by a third party. (TechEncy)
OPERATIONAL CONTROL	The day-to-day security procedures and mechanisms to protect operational systems. The operational controls consist of the physical, environmental and personnel security controls.
ON-LINE SYSTEM	Available for immediate use. Typically, it refers to being connected to the Internet or other remote service. When a user connects via modem, s/he is on-line after s/he dials in and logs-on to his/her Internet provider with his/her username and password. When a user logs-off, s/he is off-line. With cable modem and DSL service, the user is on-line all the time. A peripheral device (terminal, printer, etc.) that is turned on and connected to the computer is also on-line. (TechEncy)
OUTPUT	Data / information produced by computer processing, such as graphic display on a terminal or hard copy. (FISCAM)

TERMS	DEFINITIONS
OWNER	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. **(BPSSM)** Manager or director with responsibility for a computer resource, such as a data file or application program. (FISCAM)
OTHER SYSTEMS	Any system that is not determined to be a GSS or MA is referred to as an "Other" system.
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.
PARAMETER	A value that is given to a variable. Parameters provide a means of customizing programs. (FISCAM)
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).
PASSWORD CRACKING	The process of using password-cracking programs to identify weak passwords.
PASSWORDS	A protected string and/or character of symbols that is used to permit computer access by authenticating a particular user. A secret combination of alpha-numeric characters that a claimant memorizes and uses to authenticate his or her identity. Passwords are typically character strings. **(BPSSM)** A confidential character string used to authenticate an identity or prevent unauthorized access. (FISCAM) Most often associated with user authentication. However, they are also used to protect data and applications on many systems, including 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). (SSPS&GH - Glossary)
PENETRATION	The successful act of bypassing the security mechanisms of a system or application. **(BPSSM)** Unauthorized act of bypassing the security mechanisms of a system. (NSTISSI)

TERMS	DEFINITIONS
PENETRATION TESTING	Security testing in which evaluators attempt to circumvent the security features of a system based on their understanding of the system design and implementation. **(BPSSM)** An activity in which a test team attempts to circumvent the security processes and controls of a computer system. Posing as either internal or external unauthorized intruders (or both, in different phases of the test), the test team attempts to obtain privileged access, extract information, and demonstrate the ability to manipulate the computer in what would be unauthorized ways if it had happened outside the scope of the test.
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 IDENTIFICATION NUMBER (PIN)	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. **(ARS)**A password consisting only of decimal digits. (ARS draft v2.0)
PERSONNEL CONTROLS	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)
PERSONNEL SECURITY	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. **(BPSSM)** 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 ADP resources, which the individual will be able to access. (AISSP – Source: NISTIR 4659) (Also see Personnel Controls)
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 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 INTRUSION	Unauthorized access to or use of physical resources, including but not limited to facilities, wiring closets, and power supplies.

TERMS	DEFINITIONS
PHYSICAL SECURITY	See physical and environmental controls. **(BPSSM)** Refers to the application of physical barriers and control procedures as preventive measures and countermeasures against threats to resources and sensitive information. (SSPS&GH - Glossary) (Source: NISTIR 4659) (Also see Physical Access Control)
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.
POLICY GUIDELINE	An example of how a policy might be applied to a specific situation. An outline or checklist of detailed procedures recommended in order to satisfy a policy.
PORT	An interface between the CPU of the computer and a peripheral device that governs and synchronizes the flow of data between the CPU and the external device. (FISCAM)
POSSESSION AND CONTROL OF A TOKEN	The ability to activate and use the token in an authentication protocol.
PRACTICE STATEMENT	A formal statement of the practices followed by an authentication entity (e.g., Registration Authority, CSP, or verifier); typically, the specific steps taken to register and verify identities, issue credentials and authenticate claimants.
PRIVACY	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. **(BPSSM)** 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 so as 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 U.S.C. Section 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.
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.
PRIVATE KEY	The secret part of an asymmetric key pair that typically is used to sign or decrypt data digitally.

TERMS	DEFINITIONS
PRIVILEGES	The rights to alter, circumvent, override, or bypass the operating system or system security measures. **(BPSSM)** 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.
PROBE	Attempt to gather information about an IS or its users. (NSTISSI)
PROCEDURES	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)
PRODUCTION, INPUT / OUTPUT CONTROLS	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. **(BPSSM)** The function responsible for monitoring the information into, through, scheduling 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 ENVIRONMENT	The system environment where the agency performs its operational information processing activities. (FISCAM)
PRODUCTION PROGRAMS	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. (See Standard Profile and User Profile.) (FISCAM)
PROGRAM	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)
PROGRAM LIBRARY	See Library.
PROGRAMMER	A person, who designs, codes, tests, debugs, and documents computer programs. (FISCAM)
PROJECT OFFICER	CMS official (generally located in Central Office department) responsible for the oversight of other business partners. These include CWF Host Sites, DMERCs, standard claims processing system maintainers, Regional Laboratory Carriers, and claims processing Data Centers.
PROOF OF POSSESSION PROTOCOL (POP)	A protocol where a claimant proves to a verifier that s/he possesses and controls a token (e.g., a key or password).

TERMS	DEFINITIONS
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)
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 SERVER	A server that acts as an intermediary between two computer systems engaged in network communication. The proxy server accepts service requests to and from client computers (computers placed behind, and protected by the proxy server), and makes the connection to the desired destination on behalf of the requesting party.
PSEUDONYM	A subscriber name that has been chosen by the subscriber that is not verified as meaningful by identity proofing.
PUBLIC ACCESS CONTROLS	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	Software, which has no copyright protection and can, be used or copied by anyone free of charge. **(BPSSM)** 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	Data available to the general population. The disclosures of this information are not expected to impact the agency seriously or adversely. Examples include general organizational information on the organization's web-site, public brochures and pamphlets.
PUBLIC KEY	The public part of an asymmetric key pair that typically is used to verify signatures or encrypt data.
PUBLIC KEY CERTIFICATE	A digital document issued and signed digitally 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.
PUBLIC KEY INFRASTRUCTURE (PKI)	Framework established to issue, maintain, and revoke Public Key certificates accommodating a variety of security Technologies, including the use of software. (NSTISSI)

TERMS	DEFINITIONS
PUBLIC TRUST POSITIONS	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. (Source: 5 CFR Part 731)
QUALITY ASSURANCE	The function that reviews software project activities and tests software products throughout the software life-cycle to determine if (1) the software project is adhering to its established plans, standards, and procedures, and (2) the software meets the functional specifications defined by the user. (FISCAM)
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)
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)
RECORD	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 PROCEDURE	Actions necessary to restore data files of an IS and computational capability after a system failure. (NSTISSI)
REGISTRATION	The process through which a party applies to become a subscriber of a 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 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.
REMOTE ACCESS	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.
RESIDUAL RISK	A qualitative or quantitative substantiation of potential loss that remains after a mitigating control(s) has been implemented and is operational.

TERMS	DEFINITIONS
RESOURCE	Any function, device or collection of data in an organization that can be allocated for use by users or programs. **(BPSSM)** 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 OWNER	See Owner.
RESTORATION	The process of planning for and implementing business recovery, which enables the organization to return to a normal service level.
REVIEW AND APPROVAL	The process whereby information pertaining to the security and integrity of an ADP activity or network is collected, analyzed, and submitted to the appropriate DAA for accreditation of the activity or network.
RISK	The combination of the probability and severity of impact that results from a threat successfully breaking through a vulnerability. **(BPSSM)** The potential for harm or loss is best expressed as the answers to these four questions: What could happen? (What is the threat?) How bad could it be? (What is the impact or consequence?) How often might it happen? (What is the frequency?) How certain are the answers to the first three questions? The key element among these is the issue of uncertainty captured in the fourth question. If there is no uncertainty, there is no "risk" *per se*. (HISM)
RISK ACCEPTANCE	Formal process by which a management official agrees that no additional safeguards will be undertaken to control a specific risk.
RISK ANALYSIS	A risk analysis involves identifying the most probable threats to a system and analyzing the related vulnerabilities of the system to these threats. **(BPSSM)** The identification and study of the vulnerability of a system and the possible threats to its security. (AISSP – Source: FIPS PUB 11-3) This term represents the process of analyzing a target environment and the relationships of its risk-related attributes. The analysis should identify threat vulnerabilities, associate these vulnerabilities with affected assets, identify the potential for and nature of an undesirable result, and identify and evaluate risk-reducing countermeasures. (HISM)

TERMS	DEFINITIONS
RISK ASSESSMENT (RA)	The process of identifying, quantifying, and managing potential negative impacts on a system through qualitative or quantitative analysis. This process also identifies weak controls and provides guidance for implementing new and stronger security controls within systems. **(BPSSM)** The identification and analysis of possible risks in meeting the agency's objectives that form a basis for managing the risks identified and implementing deterrents. (FISCAM) This term represents the assignment of value to assets, threat frequency (annualized), consequence (i.e., exposure factors), and other elements of chance. The reported results of risk analysis can be said to provide an assessment or measurement of risk, regardless of the degree to which quantitative techniques are applied. The term “risk assessment” is used to characterize both the process and the result of analyzing and assessing risk. (HISM)
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). (HISM)
RISK LEVELS	The extent to which 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.

TERMS	DEFINITIONS
RISK MANAGEMENT	Process of identifying, controlling and lowering or eliminating security risks that may affect information systems, for an acceptable cost. **(BPSSM)** A management approach designed to reduce risks inherent to system development and operations. (FISCAM) The process of identifying, controlling, and eliminating or minimizing uncertain events that may affect system resources. It includes risk analysis, cost benefit analysis, selection, implementation and test, security evaluation of safeguards, and overall security review. (AISSP – Source: NISTIR 4659) This term characterizes the overall process. The first, or risk assessment, phase includes identifying risks, risk-reducing measures, and the budgetary impact of implementing decisions related to the acceptance, avoidance, or transfer of risk. The second phase of risk management includes the process of assigning priority to, budgeting, implementing, and maintaining appropriate risk-reducing measures. Risk management is a continuous process of ever-increasing complexity. (HISM)
RISK PLANNING	The process of managing a risk by initiating a risk mitigation plan that ranks, implements and maintains controls.
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)
RESEARCH AND ACKNOWLEDGEMENT	The process of acknowledging a vulnerability and researching controls to remedy the weakness.
RESOURCE	Any agency AIS asset. (AISSP – Source: DHHS Definition)
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 Systems Development Life-Cycle at CMS
ROUTERS	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. **(BPSSM)** An intermediary device on a communications network that expedites message delivery. As part of a LAN, a router receives transmitted messages and forwards them to their destination over the most efficient available route. (FISCAM)

TERMS	DEFINITIONS
RULES OF BEHAVIOR (ROB)	Guidelines describing permitted actions by users and their responsibilities when utilizing a computer system. ROB are the rules that have been established and implemented concerning use of, security in and acceptable level of risk for the system. Rules will clearly delineate responsibilities and expected behavior of all individuals with access to the system. Rules should cover such matters as work at home, dial-in access, connection to the Internet, use of copyrighted works, unofficial use of federal government equipment, the assignment and limitation of system privileges and individual accountability. (NIST SP 800-18) (SSP Methodology) **BPSSM)** Rules for individual users of each GSS or any application. These rules should clearly delineate responsibilities of and expectations for all individuals with access to the system. They should be consistent with system-specific policy as described in "An Introduction to Computer Security: The NIST Handbook" (March 16, 1995). In addition, they should state the consequences of non-compliance. The rules should be in writing and will form the basis for security awareness and training. (OMB Circular A-130)
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)
SABOTAGE	Malicious acts that can cause damage, destruction, interruption or loss of system assets. This could impact confidentiality, integrity, and availability of data**.**
SAFEGUARD	A security control or countermeasure employed to reduce the risk associated with a specific threat or group of threats **(BPSSM)** This term represents a risk-reducing measure that acts to detect, prevent, or minimize loss associated with the occurrence of a specified threat or category of threats. Safeguards are also often described as controls or countermeasures. (HISM)
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.
SANITIZATION	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.
SCANNING	The process of using software tools to identify hosts, open ports and provide information on the conditions found.

TERMS	DEFINITIONS
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".
SDLC METHODOLOGY	See System Development Life-Cycle.
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)	A commonly used protocol for managing the security of message transmission on the Internet. Often used in Internet transactions.
SECURITY	Procedures that protect organizational resources, employees and peers, paper or electronic media, hardware, software and networks from damage, theft, interruption, or change. **(BPSSM)** 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)
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 XML markup language.
SECURITY AWARENESS	The general, collective awareness of an organization's personnel on the importance of security and security controls.
SECURITY CERTIFICATION	A formal testing of the security safeguards implemented in the computer system to determine whether they meet applicable requirements and specifications. To provide more reliable technical information, certification is often performed by an independent reviewer, rather than by the people who designed the system. (NIST Special Publication 800-12)
SECURITY DOMAIN	A scope or environment of trust that shares a single security policy and a single management.
SECURITY INCIDENT	A computer security incident is any adverse event whereby some aspect of computer security could be threatened: loss of data confidentiality, disruption of data or system integrity, or disruption or Denial-of-Service.

TERMS	DEFINITIONS
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 (4) security level designations for data sensitivity and four (4) 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. (AISSP – Source: DHHS Definition)
SECURITY MANAGEMENT FUNCTION	Computer code intended to repair or lessen the impact of vulnerabilities within application software. **(BPSSM)** 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 PATCH	Computer code intended to repair or lessen the impact of vulnerabilities within application software.
SECURITY PLAN	A written plan that clearly describes the entity's security program and policies and procedures that support it. The plan and related policies should cover all major systems and facilities and outline the duties of those who are responsible for overseeing security (the security management function) as well as those who own, use, or rely on the entity's computer resources. (FISCAM)
SECURITY POLICY	The set of laws, rules and practices that regulates how an organization manages, protects, eliminates and distributes sensitive information. 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 to be a "living document", which means that the document is never finished, but is continuously updated as technology and employee requirements change. **(BPSSM)** The set of laws, rules, and practices that regulate how an Organization manages, protects, and distributes sensitive information. (NCSC-TG-004)
SECURITY PROFILE	See Profile.
SECURITY PROGRAM	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 address 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)
SECURITY REQUIREMENTS	Types and levels of protection necessary for equipment, data, information, applications, and facilities to meet security policy. (NSTISSI)

TERMS	DEFINITIONS
SECURITY REQUIREMENTS BASELINE	Description of the minimum requirements necessary for an IS to maintain an acceptable level of security. (NSTISSI)
SECURITY SOFTWARE	Software that protects data against unauthorized access. **(BPSSM)** See Access Control Software.
SECURITY SPECIFICATION	A security specification is a detailed description of the safeguards required to protect a sensitive application [or any AIS asset]. (OMB Circular A-130)
SECURITY TEST AND EVALUATION (ST&E)	An examination and analysis of the security safeguards of a system as they have been applied in an operational environment in order to determine the security posture of the system.
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 AND AWARENESS	See Information Security Training and Awareness
SENSITIVE APPLICATION	An application that processes sensitive data **(BPSSM)** 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, deliberates manipulation, (or delivery interruption) of the application. (AISSP – Source: 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	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. (AISSP – Source: OMB Circular A-130)

TERMS	DEFINITIONS
SENSITIVE INFORMATION	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 U.S.C. Section 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. **(BPSSM)** 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) 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, United States Code (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. (AISSP – Source: Computer Security Act of 1987)
SENSITIVITY OF DATA	The need to protect data from unauthorized disclosure, fraud, waste, or abuse. (SSPS&GH)
SENSITIVE MEDIA	Any form in which sensitive information is stored including paper, diskette, etc.
SENSITIVITY	The degree to which a system requires protection to ensure confidentiality, integrity and availability.
SEPARATION OF DUTIES / SEGREGATION OF DUTIES	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	A network device that provides service to the network users by managing shared resources. *Note:* This term is often used in the context of a client-server architecture for a local area network. **(BPSSM)** 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 CONTROLS	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)
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.

TERMS	DEFINITIONS
SHARED SECRET	A secret used in authentication that is known only to the claimant and the verifier.
SHOULDER SURFING	The capture via observation of information as it is entered by authorized personnel e.g., stealing phone numbers or passwords.
SIGNIFICANT CHANGE	A physical, administrative, or technical modification that alters the degree of protection required. Examples include adding a local area network, changing from batch to on-line processing, adding dial-up capability, and increasing the equipment capacity of the installation. (AISSP – Source: DHHS 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 = SINGLE LOSS EXPECTANCY The SLE is usually an end 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. (HISM)
SMART CARD	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 PIN. **(BPSSM)** A credit card sized token that contains a microprocessor and memory circuits for authenticating a user of computer, banking, or transportation services. (FISCAM)
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)
SOCIAL ENGINEERING	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.
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. **(BPSSM)** A computer program or programs, in contrast to the physical environment on which programs run (hardware). (FISCAM)

TERMS	DEFINITIONS
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)
SPOOFING	An attack in which an unauthorized person or process pretends to be an authorized person or process.
SSPS&G HANDBOOK	Systems Security Policy Standards and Guidelines Handbook
STAND-ALONE SYSTEM	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	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; and A degree or level of required excellence or attainment. 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. **(BPSSM)** In computing, a set of detailed technical guidelines used as a means of establishing uniformity in an area of hardware or software development. (FISCAM)
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)
SUBJECT	The person whose identity is bound in a particular credential.
SUBSCRIBER	A party who receives a credential or token from a CSP and becomes a claimant in an authentication protocol.
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.

TERMS	DEFINITIONS
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.
SYSTEM	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) A set of information resources under the same management control that share common functionality and require the same level of security controls. The phase "General Support Systems (GSS)" as used in OMB Circular A-130, Appendix III, is replaced in this document with "system" for easy readability. A "system" includes "Major Applications (MA)," as used in OMB Circular A-130, Appendix III, (e.g., payroll and personnel program software, control software, or software for command and control). 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. 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 (CMS, System Security Plans (SSP) Methodology, July 2000, SSPM.
SYSTEM ACCESS CONTROL	See Access Control
SYSTEM ADMINISTRATOR	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 BIOS	The basic program that handles instructions, and interfaces to initialize and operate input and output procedures for computer hardware.
SYSTEM DEVELOPMENT LIFE-CYCLE (SDLC)	The period of time that begins when a system is conceived and ends when the system is no longer available for use. 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. (FIPS PUB 101, SSP Methodology) **(BPSSM)** The policies and procedures that govern software development and modification as a software product goes through each phase of its life-cycle. (FISCAM)

TERMS	DEFINITIONS
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 GSS, MA, or "Other" system.
SYSTEM IMPACT	The degree of harm or potential harm caused to a system.
SYSTEM INTERCONNECTION / INFORMATION SHARING	The direct connection between various systems for the purpose of sharing information resources.
SYSTEM INTERFACE	A shared boundary where interaction occurs; i.e., the boundary between two or more subsystems or devices.
SYSTEM LIFE-CYCLE	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 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. (AISSP – Source: FIPS PUB 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)
SYSTEM OPERATIONAL STATUS	*New* (The status of a development effort with the objective of producing a system which has not previously been implemented at CMS). *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 which 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.

TERMS	DEFINITIONS
SYSTEM OWNER / MANAGER	The individual at CMS who serves as the primary point of contact for the system being developed or maintained. The System Owner / Manager has true ownership and fiduciary responsibility for the system, especially from both a Privacy Act and System Security standpoint, and is therefore generally at the Director or Deputy Director level. **(BPSSM)** The official who is responsible for the operation and use of an automated information system. (AISSP – Source: DHHS Definition)
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. (AISSP – Source: FIPS PUB 11-3)
SYSTEM SOFTWARE	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 SECURITY ADMINISTRATOR (SSA)	The person responsible for administering security on a multi-user computer system, communications system, or both.
SYSTEM SECURITY COORDINATOR (SSC)	Term used to designate the security officer in the 1992 ROM, MIM, and MCM. This business partner security officer had complete oversight and responsibility for all aspects of the security of the Medicare program.
SYSTEM SECURITY INCIDENTS (BREACHES)	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. (SSPS&GH – Glossary)
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)	A document that provides an overview of the security requirements of the system describes controls in place to meet those requirements and delineates responsibilities and expected behavior of all individuals who access the system. **(BPSSM)** Provides a basic overview of the security and privacy requirements of the subject system and the agency's plan for meeting those requirements. (AISSP) (OMB Bulletin 90-08) (Also see IS Security Plan and System Security Plan)

TERMS	DEFINITIONS
SYSTEM SECURITY PROFILE	Detailed security description of the physical structure, equipment component, location, relationships, and general operating environment of an IS. (NSTISSI)
SYSTEM TESTING	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)
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)
TECHNICAL CONTROLS	A software measure that ensures the confidentiality, integrity and availability of a system and/or data. **(BPSSM)** See Logical Access Control.
TELECOMMUNICATIONS	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)
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 BED	Test environment containing the software, data, and simulations necessary for testing systems.
THREAT	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. **(BPSSM)** Any circumstance or event with the potential to cause harm to a system in the form of destruction, disclosure, modification of data, and/or Denial-of-Service. (NCSC-TG-004) This term defines an event (e.g., a tornado, theft, or computer virus infection), the occurrence of which could have an undesirable impact. (HISM)
THREAT ANALYSIS	The examination of all actions and events that might affect a system or operation adversely. (NCSC-TG-004) This task includes the identification of threats that may impact the target environment adversely. (HISM)

TERMS	DEFINITIONS
TOKEN	A physical device used to convey privilege or a capability, e.g., a handheld password generator. **(BPSSM)** 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) **(ARS)** Something that the claimant possesses and controls (typically a key or password) used to authenticate the claimant’s identity. (ARS draft v2.0)
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.
TRAINING AND AWARENESS	See Information Security Training and Awareness.
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)
TRANSPORT LAYER SECURITY (TLS)	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 Socket Layer (SSL) protocol and is effectively SSL version 3.1.
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)
TROJAN HORSE	A computer program with an apparent or actual useful function that contains additional, malicious, and hidden functions. **(BPSSM)** A computer program that conceals harmful code. A “Trojan horse” usually masquerades as a useful program that a user would wish to execute. (FISCAM) A destructive program disguised as a game, a utility, or an application. When run, a Trojan horse does something devious to the computer system while appearing to do something useful. (AISSP – Source: *Microsoft Press Computer Dictionary*)

TERMS	DEFINITIONS
TUNNELED PASSWORD PROTOCOL	A protocol where a password is sent through a protected channel. For example, the TLS protocol is often used with a verifier's public key certificate to: (1) authenticate the verifier to the claimant; (2) establish an encrypted session between the verifier and claimant; and (3) transmit the claimant's password to the verifier. The encrypted TLS session protects the claimant's password from eavesdroppers.
UNAUTHORIZED DISCLOSURE	Exposure of information to individuals not authorized to receive it. (NSTISSI)
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. (HISM)
UNCLASSFIED	Information that is designated as neither sensitive nor classified. The public release of this information does not violate national security interests. **BPSSM)** 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. (NSTISSI)
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)
UPDATE ACCESS	This access level includes the ability to change data or a software program. (FISCAM)
USER	The person who uses a computer system and its application programs to perform tasks and produce results. (FISCAM) 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. (AISSP – Source: OMB Circular A-130)
USER IDENTIFICATION (UID)	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)

TERMS	DEFINITIONS
VALIDATION CONTROLS	Controls, tests and evaluations that assess the level of compliance with security specifications and requirements. **(BPSSM)** 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)
VERIFIED NAME	A subscriber name that has been verified by identity proofing.
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.
VIRTUAL PRIVATE NETWORKS (VPN)	A combination of tunneling, encryption, authentication, and access control technologies and services used to carry traffic over the Internet, a managed IP network, or a provider's backbone network to ensure the security of information transmitted.
VIRUS	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. 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. **(BPSSM)** A program that "infects" computer files, usually executable programs, by inserting a copy of itself into the file. These copies are usually executed when the "infected" file is loaded into memory, allowing the virus to infect other files. Unlike the computer worm, a virus requires human involvement (usually unwitting) to propagate. (FISCAM) A self-propagating Trojan horse composed of a mission component, a trigger component, and a self-propagating component. (NCSC-TG-004)
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.

TERMS	DEFINITIONS
VULNERABILITY	A weakness in system security procedures, system design, implementation, controls, and configurations that could be breached to violate system security policy. **(BPSSM)** This term characterizes the absence or weakness of a risk-reducing safeguard. It is a condition that has the potential to allow a threat to occur with greater frequency, greater impact, or both. For example, not having a fire suppression system could allow an otherwise minor, easily quenched fire to become a catastrophic fire. Both expected frequency (ARO) and exposure factor (EF) for fire are increased as a consequence of not having a fire suppression system. (HISM)
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	A measurement of vulnerability that includes the susceptibility of a particular system to a specific attack and the opportunities that are available to a threat agent to mount that attack.
WARNING BANNER	Primary definition: A notice presented prior to authentication to a 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. An additional definition (example): NIST Special Publication 800-12 Footnote 131: The Department of Justice has advised that an ambiguity in U.S. law makes it unclear whether keystroke monitoring is considered equivalent to an unauthorized telephone wiretap. The ambiguity results from the fact that current laws were written years before such concerns as keystroke monitoring or system intruders became prevalent. Additionally, no legal precedent has been set to determine whether keystroke monitoring is legal or illegal. System administrators conducting such monitoring might be subject to criminal and civil liabilities. The Department of Justice advises system administrators to protect themselves by giving notice to system users if keystroke monitoring is being conducted. Notice should include agency/organization policy statements, training on the subject, and a "banner" notice on each system being monitored. [NIST, *CSL Bulletin*, March 1993]
WIDE AREA NETWORK (WAN)	A group of computers and other devices dispersed over a wide geographical area and connected by communications links. (FISCAM) A communications network that connects geographically separated areas. (AISSP – Source: *Microsoft Press Computer Dictionary*)
WORKSTATION	A microcomputer or terminal connected to a network. "Workstation" can also refer to a powerful, stand-alone computer with considerable calculating or graphics capability. (FISCAM)

TERMS	DEFINITIONS
WORM	An independent program that reproduces by copying itself from one system to another while traveling from machine to machine across network connections. **(BPSSM)** An independent computer Program that reproduces by copying itself from one system to another across a network. Unlike computer viruses, worms do not require human involvement to propagate. (FISCAM) 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. (AISSP – Source: *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. (NSTISSI)
WRITE ACCESS	Permission to write to an object in an IS. (NSTISSI)
ZERO KNOWLEDGE PASSWORD	Strong password used with special “zero knowledge” protocol.
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.