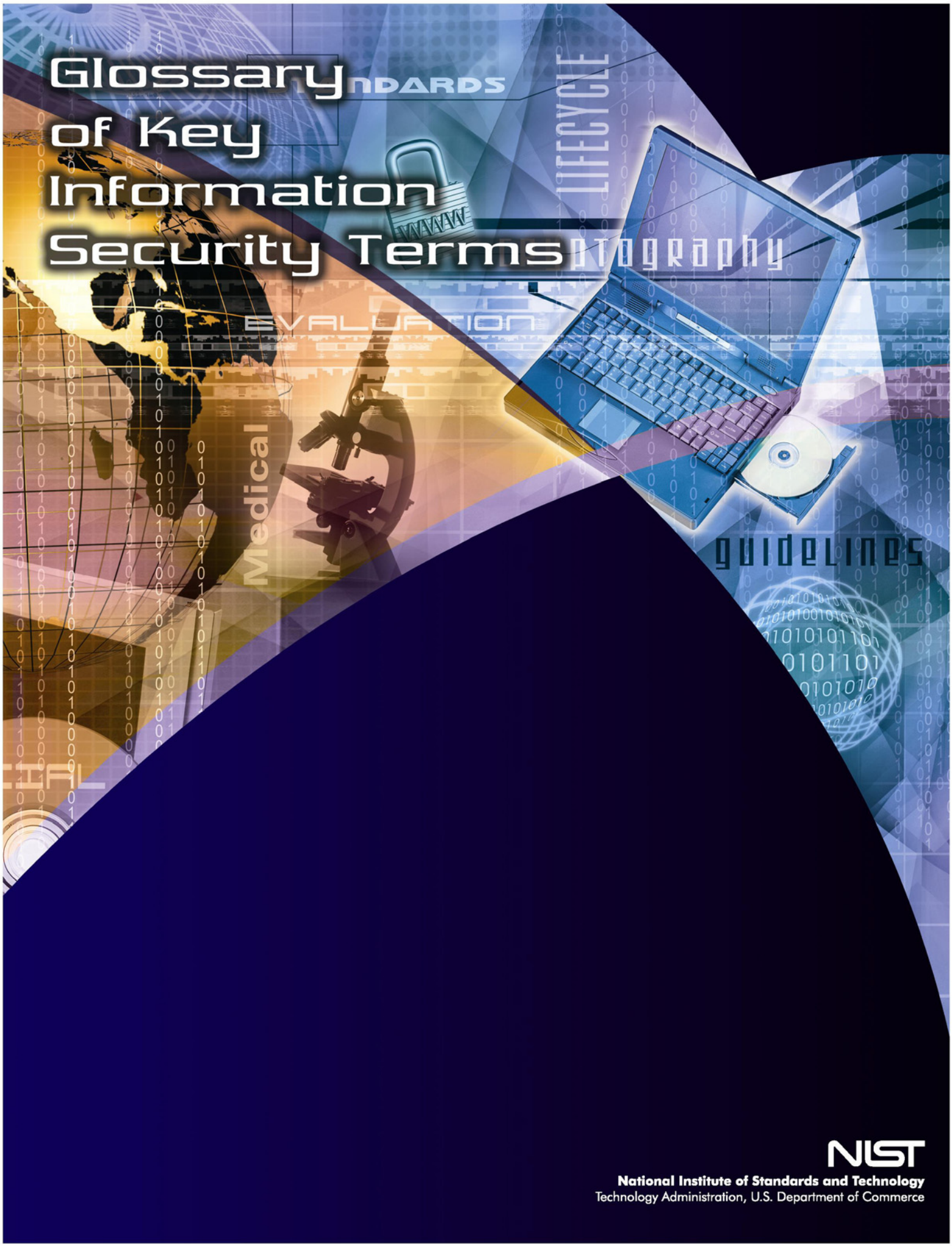
Glossary of Key Information Security Terms



NIST
National Institute of Standards and Technology
Technology Administration, U.S. Department of Commerce

NIST IR 7298

Glossary of Key Information Security Terms

Richard Kissel, editor

April 25, 2006

U.S. Department of Commerce
Carlos M. Gutierrez, Secretary

Technology Administration
Robert Cresanti, Under Secretary of Commerce for Technology

National Institute of Standards and Technology
William Jeffrey, Director

Introduction

We have received numerous requests to provide a summary glossary for our publications and make it available to practitioners. As a result of those requests, this glossary of ***basic*** security terms has been extracted from NIST Federal Information Processing Standards (FIPS) and the Special Publication (SP) 800 series. The terms included are ***not all inclusive*** of terms found in these publications, but are a ***subset of basic terms*** that are most frequently used. The purpose of this glossary is to provide a central resource of definitions most commonly used in NIST security publications.

Each entry in the glossary points to one or more source NIST publications, and in addition, supplemental sources where appropriate. A list of the supplemental (non-NIST) sources may be found on pages 85-86. As we are continuously refreshing our publication suite, terms included in the glossary come from our more recent publications and existing FIPS.

It is our intention to keep the glossary current by providing updates online. New definitions will be added to the glossary, as required, and updated versions will be posted to the Computer Security Resource Center (CSRC) Web site at http://csrc.nist.gov/.

Comments and suggestions on this publication should be sent to secglossary@nist.gov.

Access –	Ability to make use of any information system (IS) resource. SOURCE: SP 800-32
Access Authority –	An entity responsible for monitoring and granting access privileges for other authorized entities. SOURCE: SP 800-57
Access Control –	The process of granting or denying specific requests: 1) for obtaining and using information and related information processing services; and 2) to enter specific physical facilities (e.g., Federal buildings, military establishments, and border crossing entrances). SOURCE: FIPS 201
Access Control Lists – (ACLs)	A register of: 1) users (including groups, machines, processes) who have been given permission to use a particular system resource, and 2) the types of access they have been permitted. SOURCE: SP 800-12
Account Management, User –	Involves 1) the process of requesting, establishing, issuing, and closing user accounts; 2) tracking users and their respective access authorizations; and 3) managing these functions. SOURCE: SP 800-12
Accountability –	The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports non-repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action. SOURCE: SP 800-27A
Accreditation –	The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls. SOURCE: SP 800-53; FIPS 200
Accreditation Authority –	SEE Authorizing Official
Accreditation Boundary –	All components of an information system to be accredited by an authorizing official and excludes separately accredited systems, to which the information system is connected. SOURCE: SP 800-53

Accreditation Package –	The evidence provided to the authorizing official to be used in the security accreditation decision process. Evidence includes, but is not limited to: 1) the system security plan; 2) the assessment results from the security certification; and 3) the plan of action and milestones. SOURCE: SP 800-37
Accrediting Authority –	Official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals. SOURCE: SP 800-53
Activation Data –	Private data, other than keys, that are required to access cryptographic modules. SOURCE: SP 800-32
Active Content –	Active content refers to electronic documents that are able to automatically carry out or trigger actions on a computer platform without the intervention of a user. SOURCE: SP 800-46
Adequate Security –	Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information. SOURCE: SP 800-53; FIPS 200; OMB Circular A-130, App. III
Administrative Safeguards –	Administrative actions, policies, and procedures to manage the selection, development, implementation, and maintenance of security measures to protect electronic health information and to manage the conduct of the covered entity's workforce in relation to protecting that information. SOURCE: SP 800-66
Advanced Encryption Standard – (AES)	The Advanced Encryption Standard specifies a U.S. Government-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. SOURCE: SP 800-46 This standard specifies the Rijndael algorithm, a symmetric block cipher that can process data blocks of 128 bits, using cipher keys with lengths of 128, 192, and 256 bits. SOURCE: FIPS 197

Agency –	Any executive department, military department, government corporation, government controlled corporation, or other establishment in the executive branch of the government (including the Executive Office of the President), or any independent regulatory agency, but does not include: 1) the General Accounting Office; 2) the Federal Election Commission; 3) the governments of the District of Columbia and of the territories and possessions of the United States, and their various subdivisions; or 4) government-owned contractor-operated facilities, including laboratories engaged in national defense research and production activities. SOURCE: FIPS 200; 44 U.S.C., Sec. 3502 ALSO SEE Executive Agency
Agency Certification Authority – (CA)	A CA that acts on behalf of an Agency, and is under the operational control of an Agency. SOURCE: SP 800-32
Agent –	A program used in distributed denial of service (DDoS) attacks that sends malicious traffic to hosts based on the instructions of a handler. SOURCE: SP 800-61
Analysis –	The examination of acquired data for its significance and probative value to the case. SOURCE: SP 800-72
Antivirus Software –	A program that monitors a computer or network to identify all major types of malware and prevent or contain malware incidents. SOURCE: SP 800-83
Applicant –	The subscriber is sometimes called an "applicant" after applying to a certification authority for a certificate, but before the certificate issuance procedure is completed. SOURCE: SP 800-32
Application –	The use of information resources (information and information technology) to satisfy a specific set of user requirements. SOURCE: SP 800-37
Application Content Filtering –	Application content filtering is performed by a software proxy agent to remove or quarantine viruses that may be contained in email attachments, to block specific Multipurpose Internet Mail Extensions (MIME) types, or to filter other active content such as Java, JavaScript, and ActiveX® Controls. SOURCE: SP 800-41

Approved –	Federal Information Processing Standard (FIPS) approved or National Institute of Standards and Technology (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. SOURCE: FIPS 201 FIPS-approved and/or NIST-recommended. SOURCE: FIPS 140-2
Approved Mode of Operation –	A mode of the cryptographic module that employs only Approved security functions (not to be confused with a specific mode of an Approved security function, e.g., Data Encryption Standard (DES) Cipher Block Chaining (CBC) mode). SOURCE: FIPS 140-2
Approved Security Function –	A security function (e.g., cryptographic algorithm, cryptographic key management technique, or authentication technique) that is either a) specified in an Approved standard, b) adopted in an Approved standard and specified either in an appendix of the Approved standard or in a document referenced by the Approved standard, or c) specified in the list of Approved security functions. SOURCE: FIPS 140-2
Assessment Method –	A focused activity or action employed by an assessor for evaluating a particular attribute of a security control. SOURCE: SP 800-53
Assessment Procedure –	A set of activities or actions employed by an assessor to determine the extent to which a security control is implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. SOURCE: SP 800-53
Asset –	A major application, general support system, high impact program, physical plant, mission critical system, or a logically related group of systems. SOURCE: SP 800-26

Assurance –	One of the five "Security Goals." It involves support for our confidence that the other four security goals (integrity, availability, confidentiality, and accountability) have been adequately met by a specific implementation. "Adequately met" includes (1) functionality that performs correctly, (2) sufficient protection against unintentional errors (by users or software), and (3) sufficient resistance to intentional penetration or by-pass. SOURCE: SP 800-27A
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. SOURCE: FIPS 201
Attack Signature –	A specific sequence of events indicative of an unauthorized access attempt. SOURCE: SP 800-12
Attribute Authority –	An entity, recognized by the Federal Public Key Infrastructure (PKI) Policy Authority or comparable Agency body as having the authority to verify the association of attributes to an identity. SOURCE: SP 800-32
Audit –	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 SOURCE: SP 800-32; CNSSI-4009
Audit Data –	Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event. SOURCE: SP 800-32
Audit Reduction Tools –	Preprocessors designed to reduce the volume of audit records to facilitate manual review. Before a security review, these tools can remove many audit records known to have little security significance. These tools generally remove records generated by specified classes of events, such as records generated by nightly backups. SOURCE: SP 800-12
Audit Trail –	A record showing who has accessed an Information Technology (IT) system and what operations the user has performed during a given period. SOURCE: SP 800-47

Authenticate – To confirm the identity of an entity when that identity is presented.

SOURCE: SP 800-32

Authentication – Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

SOURCE: SP 800-53; FIPS 200

The process of establishing confidence of authenticity.

SOURCE: FIPS 201

Encompasses identity verification, message origin authentication, and message content authentication.

SOURCE: FIPS 190

A process that establishes the origin of information or determines an entity's identity.

SOURCE: SP 800-21 [2nd Ed]

Authentication Code – A cryptographic checksum based on an Approved security function (also known as a Message Authentication Code (MAC)).

SOURCE: FIPS 140-2

Authentication, Electronic – The process of establishing confidence in user identities electronically presented to an information system.

SOURCE: SP 800-63

Authentication Mechanism – Hardware or software-based mechanisms that force users to prove their identity before accessing data on a device.

SOURCE: SP 800-72

Authentication Mode – A block cipher mode of operation that can provide assurance of the authenticity and, therefore, the integrity of data.

SOURCE: SP 800-38B

Authentication Protocol – A well specified message exchange process that verifies possession of a token to remotely authenticate a claimant. Some authentication protocols also generate cryptographic keys that are used to protect an entire session, so that the data transferred in the session is cryptographically protected.

SOURCE: SP 800-63

Authentication Tag – A pair of bit strings associated to data to provide assurance of its authenticity.

SOURCE: SP 800-38B

Authentication Token – Authentication information conveyed during an authentication exchange.

SOURCE: FIPS 196

Authenticity – The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. See authentication.

SOURCE: SP 800-53

Authorization – The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.

SOURCE: SP 800-37

Authorize Processing – The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.

SOURCE: SP 800-53

Authorizing Official – Official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals. Synonymous with Accreditation Authority.

SOURCE: SP 800-53; FIPS 200

Authorizing Official – Designated Representative – Individual selected by an authorizing official to act on their behalf in coordinating and carrying out the necessary activities required during the security certification and accreditation of an information system.

SOURCE: SP 800-37

Automated Key Transport – The transport of cryptographic keys, usually in encrypted form, using electronic means such as a computer network (e.g., key transport/agreement protocols).

SOURCE: FIPS 140-2

Automated Password Generator – An algorithm which creates random passwords that have no association with a particular user.

SOURCE: FIPS 181

Availability – Ensuring timely and reliable access to and use of information.

SOURCE: SP 800-53; FIPS 200; FIPS 199; 44 U.S.C., Sec. 3542

Awareness (Information Security) – Activities which seek to focus an individual's attention on an (information security) issue or set of issues.

SOURCE: SP 800-50

Backup – A copy of files and programs made to facilitate recovery if necessary.

SOURCE: SP 800-34; CNSSI-4009

Baseline Security – The minimum security controls required for safeguarding an IT system based on its identified needs for confidentiality, integrity and/or availability protection.

SOURCE: SP 800-16

Baselining – Monitoring resources to determine typical utilization patterns so that significant deviations can be detected.

SOURCE: SP 800-61

Bastion Host – A bastion host is typically a firewall implemented on top of an operating system that has been specially configured and hardened to be resistant to attack.

SOURCE: SP 800-41

Behavioral Outcome – What an individual who has completed the specific training module is expected to be able to accomplish in terms of IT security-related job performance.

SOURCE: SP 800-16

Binding – Process of associating two related elements of information.

SOURCE: SP 800-32

An acknowledgement by a trusted third party that associates an entity's identity with its public key. This may take place through (1) a certification authority's generation of a public key certificate, (2) a security officer's verification of an entity's credentials and placement of the entity's public key and identifier in a secure database, or (3) an analogous method.

SOURCE: SP 800-21 [2nd Ed]

Biometric – A physical or behavioral characteristic of a human being.

SOURCE: SP 800-32

A measurable, physical characteristic or personal behavioral trait used to recognize the identity, or verify the claimed identity, of an applicant. Facial images, fingerprints, and handwriting samples are all examples of biometrics.

SOURCE: FIPS 201

Biometric Information – The stored electronic information pertaining to a biometric. This information can be in terms of raw or compressed pixels or in terms of some characteristic (e.g. patterns.)

SOURCE: FIPS 201

Biometric System – An automated system capable of:
1) capturing a biometric sample from an end user;
2) extracting biometric data from that sample;
3) comparing the biometric data with that contained in one or more reference templates;
4) deciding how well they match; and
5) indicating whether or not an identification or verification of identity has been achieved.

SOURCE: FIPS 201

Biometric Template – A characteristic of biometric information (e.g. minutiae or patterns.)

SOURCE: FIPS 201

Blended Attack – Malicious code that uses multiple methods to spread.

SOURCE: SP 800-61

Block – Sequence of binary bits that comprise the input, output, State, and Round Key. The length of a sequence is the number of bits it contains. Blocks are also interpreted as arrays of bytes.

SOURCE: FIPS 197

Block Cipher – A symmetric key cryptographic algorithm that transforms a block of information at a time using a cryptographic key. For a block cipher algorithm, the length of the input block is the same as the length of the output block.

SOURCE: SP 800-90

Block Cipher Algorithm – A family of functions and their inverses that is parameterized by a cryptographic key; the function maps bit strings of a fixed length to bit strings of the same length.

SOURCE: SP 800-67

Boot Sector Virus – A virus that plants itself in a system's boot sector and infects the master boot record.

SOURCE: SP 800-61

Boundary Protection –	Monitoring and control of communications at the external boundary between information systems completely under the management and control of the organization and information systems not completely under the management and control of the organization, and at key internal boundaries between information systems completely under the management and control of the organization, to prevent and detect malicious and other unauthorized communication, employing controlled interfaces (e.g., proxies, gateways, routers, firewalls, encrypted tunnels). SOURCE: SP 800-53 Rev 1
Boundary Router –	A boundary router is located at the organizations boundary to an external network. SOURCE: SP 800-41
Brute Force Password Attack –	A method of accessing an obstructed device through attempting multiple combinations of numeric and/or alphanumeric passwords. SOURCE: SP 800-72
Buffer Overflow –	A condition at an interface under which more input can be placed into a buffer or data holding area than the capacity allocated, overwriting other information. Attackers exploit such a condition to crash a system or to insert specially crafted code that allows them to gain control of the system. SOURCE: SP 800-28
Buffer Overflow Attack –	A method of overloading a predefined amount of space in a buffer, which can potentially overwrite and corrupt data in memory. SOURCE: SP 800-72
Business Continuity Plan – (BCP)	The documentation of a predetermined set of instructions or procedures that describe how an organization's business functions will be sustained during and after a significant disruption. SOURCE: SP 800-34
Business Impact Analysis – (BIA)	An analysis of an information technology (IT) system's requirements, processes, and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption. SOURCE: SP 800-34
Business Recovery-Resumption Plan – (BRP)	The documentation of a predetermined set of instructions or procedures that describe how business processes will be restored after a significant disruption has occurred. SOURCE: SP 800-34

Capture – The method of taking a biometric sample from an end user.

Source: FIPS 201

Cardholder – An individual possessing an issued Personal Identity Verification (PIV) card.

Source: FIPS 201

CBC/MAC – SEE Cipher Block Chaining-Message Authentication Code

CCM – SEE Counter with Cipher-Block Chaining-Message Authentication Code

Certificate – A digital representation of information which at least
1) identifies the certification authority issuing it,
2) names or identifies its subscriber,
3) contains the subscriber's public key,
4) identifies its operational period, and
5) is digitally signed by the certification authority issuing it.

SOURCE: SP 800-32

A set of data that uniquely identifies an entity, contains the entity's public key and possibly other information, and is digitally signed by a trusted party, thereby binding the public key to the entity. Additional information in the certificate could specify how the key is used and its cryptoperiod.

SOURCE: SP 800-21 [2nd Ed]

Certificate Management Authority – (CMA) A Certification Authority (CA) or a Registration Authority (RA).

SOURCE: SP 800-32

Certificate Policy – (CP) A Certificate Policy is a specialized form of administrative policy tuned to electronic transactions performed during certificate management. A Certificate Policy addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery and administration of digital certificates. Indirectly, a certificate policy can also govern the transactions conducted using a communications system protected by a certificate-based security system. By controlling critical certificate extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications.

SOURCE: SP 800-32

Certificate-Related Information – Information, such as a subscriber's postal address, that is not included in a certificate. May be used by a Certification Authority (CA) managing certificates.

SOURCE: SP 800-32

Certificate Revocation List – (CRL)	A list of revoked public key certificates created and digitally signed by a Certification Authority. SOURCE: SP 800-63 A list of revoked but un-expired certificates issued by a CA. SOURCE: SP 800-21 [2nd Ed]
Certificate Status Authority –	A trusted entity that provides on-line verification to a Relying Party of a subject certificate's trustworthiness, and may also provide additional attribute information for the subject certificate. SOURCE: SP 800-32
Certification –	A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. SOURCE: SP 800-53; FIPS 200 The process of verifying the correctness of a statement or claim and issuing a certificate as to its correctness. SOURCE: FIPS 201
Certification Agent –	The individual, group, or organization responsible for conducting a security certification. SOURCE: SP 800-53
Certification and Accreditation – (C&A)	A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. *Accreditation* is the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls. SOURCE: SP 800-37
Certification Authority – (CA)	A trusted entity that issues and revokes public key certificates. SOURCE: FIPS 201

	The entity in a public key infrastructure (PKI) that is responsible for issuing certificates and exacting compliance to a PKI policy. SOURCE: SP 800-21 [2nd Ed]
Certification Authority Facility –	The collection of equipment, personnel, procedures and structures that are used by a Certification Authority to perform certificate issuance and revocation. SOURCE: SP 800-32
Certification Practice Statement – (CPS)	A statement of the practices that a Certification Authority employs in issuing, suspending, revoking and renewing certificates and providing access to them, in accordance with specific requirements (i.e., requirements specified in this Certificate Policy, or requirements specified in a contract for services). SOURCE: SP 800-32
Chain of Custody –	A process that tracks the movement of evidence through its collection, safeguarding, and analysis lifecycle by documenting each person who handled the evidence, the date/time it was collected or transferred, and the purpose for the transfer. SOURCE: SP 800-72
Challenge-Response Protocol –	An authentication protocol where the verifier sends the claimant a challenge (usually a random value or a nonce) that the claimant combines with a shared secret (often by hashing the challenge and secret together) to generate a response that is sent to the verifier. The verifier knows the shared secret and can independently 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 successfully authenticated himself. 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 directly intercept the password itself, but the eavesdropper may be able to find the password with an off-line password guessing attack. SOURCE: SP 800-63

Chief Information Officer – (CIO)	Agency official responsible for: 1) Providing advice and other assistance to the head of the executive agency and other senior management personnel of the agency to ensure that information technology is acquired and information resources are managed in a manner that is consistent with laws, executive orders, directives, policies, regulations, and priorities established by the head of the agency; 2) Developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture for the agency; and 3) Promoting the effective and efficient design and operation of all major information resources management processes for the agency, including improvements to work processes of the agency. SOURCE: SP 800-53; FIPS 200; Public Law 104-106, Sec. 5125(b)
Chief Information Security Officer –	SEE Senior Agency Information Security Officer.
Cipher –	Series of transformations that converts plaintext to ciphertext using the Cipher Key. SOURCE: FIPS 197
Cipher Block Chaining-Message Authentication Code – (CBC-MAC)	A secret-key block-cipher algorithm used to encrypt data and to generate a Message Authentication Code (MAC) to provide assurance that the payload and the associated data are authentic. SOURCE: SP 800-38C
Cipher Key –	Secret, cryptographic key that is used by the Key Expansion routine to generate a set of Round Keys; can be pictured as a rectangular array of bytes, having four rows and Nk columns. SOURCE: FIPS 197
Cipher Suite –	Negotiated algorithm identifiers. Cipher suites are identified in human readable form using a pneumonic code. SOURCE: SP 800-52
Ciphertext –	Data output from the Cipher or input to the Inverse Cipher. SOURCE: FIPS 197 Data in its encrypted form. SOURCE: SP 800-21 [2nd Ed]
Claimant –	A party whose identity is to be verified using an authentication protocol. SOURCE: SP 800-63; FIPS 201

An entity which is or represents a principal for the purposes of authentication, together with the functions involved in an authentication exchange on behalf of that entity. A claimant acting on behalf of a principal must include the functions necessary for engaging in an authentication exchange. (e.g., a smartcard (claimant) can act on behalf of a human user (principal))

SOURCE: FIPS 196

Classified Information – Information that has been determined pursuant to Executive Order (E.O.) 13292 or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

SOURCE: SP 800-60; E.O. 13292

Client (Application) – A system entity, usually a computer process acting on behalf of a human user, that makes use of a service provided by a server.

SOURCE: SP 800-32

Clinger-Cohen Act of 1996 – Also known as Information Technology Management Reform Act. A statute that substantially revised the way that IT resources are managed and procured, including a requirement that each agency design and implement a process for maximizing the value and assessing and managing the risks of IT investments.

SOURCE: SP 800-64

Cold Site – A backup facility that has the necessary electrical and physical components of a computer facility, but does not have the computer equipment in place. The site is ready to receive the necessary replacement computer equipment in the event that the user has to move from their main computing location to an alternate site.

SOURCE: SP 800-34

Collision – Two or more distinct inputs produce the same output.

SOURCE: SP 800-57

Common Security Control – Security control that can be applied to one or more agency information systems and has the following properties:

1) the development, implementation, and assessment of the control can be assigned to a responsible official or organizational element (other than the information system owner); and
2) the results from the assessment of the control can be used to support the security certification and accreditation processes of an agency information system where that control has been applied.

SOURCE: SP 800-53; FIPS 200

Common Vulnerabilities and Exposures – (CVE)	A dictionary of common names for publicly known IT system vulnerabilities. SOURCE: SP 800-51
Comparison –	The process of comparing a biometric with a previously stored reference template or templates. SOURCE: FIPS 201
Compensating Controls –	The management, operational, and technical controls (i.e., safeguards or countermeasures) employed by an organization in lieu of the recommended controls in the low, moderate, or high security control baselines, that provide equivalent or comparable protection for an information system. SOURCE: FIPS 200
Compensating Security Controls –	The management, operational, and technical controls (i.e., safeguards or countermeasures) employed by an organization in lieu of the recommended controls in the low, moderate, or high baselines described in NIST Special Publication 800-53, that provide equivalent or comparable protection for an information system. SOURCE: SP 800-53
Compromise –	Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred. SOURCE: SP 800-32 The unauthorized disclosure, modification, substitution or use of sensitive data (including plaintext cryptographic keys and other critical security parameters). SOURCE: FIPS 140-2
Computer Forensics –	The practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data. SOURCE: SP 800-61
Computer Security Incident –	A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. SOURCE: SP 800-61

Computer Security Incident Response Team – (CSIRT)	A capability set up for the purpose of assisting in responding to computer security-related incidents; also called a Computer Incident Response Team (CIRT) or a CIRC (Computer Incident Response Center, Computer Incident Response Capability). SOURCE: SP 800-61
Computer Security Object – (CSO)	A resource, tool, or mechanism used to maintain a condition of security in a computerized environment. These objects are defined in terms of attributes they possess, operations they perform or are performed on them, and their relationship with other objects. SOURCE: FIPS 188
Computer Security Objects Register –	A collection of Computer Security Object names and definitions kept by a registration authority. SOURCE: FIPS 188
Computer Virus –	A computer virus is similar to a Trojan horse because it is a program that contains hidden code, which usually performs some unwanted function as a side effect. The main difference between a virus and a Trojan horse is that the hidden code in a computer virus can only replicate by attaching a copy of itself to other programs and may also include an additional "payload" that triggers when specific conditions are met. SOURCE: SP 800-46
Confidentiality –	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. SOURCE: SP 800-53; FIPS 200; FIPS 199; 44 U.S.C., Sec. 3542 The property that sensitive information is not disclosed to unauthorized individuals, entities or processes. SOURCE: FIPS 140-2
Configuration Control –	Process for controlling modifications to hardware, firmware, software, and documentation to ensure the information system is protected against improper modifications prior to, during, and after system implementation. SOURCE: SP 800-53; CNSSI-4009
Contingency Plan –	Management policy and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disaster. SOURCE: SP 800-34

Continuity of Operations Plan – (COOP)	A predetermined set of instructions or procedures that describe how an organization's essential functions will be sustained for up to 30 days as a result of a disaster event before returning to normal operations. SOURCE: SP 800-34
Continuity of Support Plan –	The documentation of a predetermined set of instructions or procedures mandated by Office of Management and Budget (OMB) A-130 that describe how to sustain major applications and general support systems in the event of a significant disruption. SOURCE: SP 800-34
Control Information –	Information that is entered into a cryptographic module for the purposes of directing the operation of the module. SOURCE: FIPS 140-2
Controlled Interface –	Mechanism that facilitates the adjudication of different interconnected system security policies (e.g., controlling the flow of information into or out of an interconnected system). SOURCE: SP 800-53; FIPS 200; CNSSI-4009
Cookie –	A piece of information supplied by a web server to a browser, along with requested resource, for the browser to store temporarily and return to the server on any subsequent visits or requests. SOURCE: SP 800-46
Counter with Cipher Block Chaining-Message Authentication Code – (CCM)	A mode of operation for a symmetric key block cipher algorithm. It combines the techniques of the Counter (CTR) mode and the Cipher Block Chaining-Message Authentication Code (CBC-MAC) algorithm to provide assurance of the confidentiality and the authenticity of computer data. SOURCE: SP 800-38C
Countermeasures –	Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system. Synonymous with security controls and safeguards. SOURCE: SP 800-53; FIPS 200; CNSSI-4009
Credential –	An object that authoritatively binds an identity (and optionally, additional attributes) to a token possessed and controlled by a person. SOURCE: SP 800-63 Evidence attesting to one's right to credit or authority. SOURCE: FIPS 201

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. SOURCE: SP 800-63
Critical Security Parameter –	Security-related information (e.g., secret and private cryptographic keys, and authentication data such as passwords and Personal Identification Numbers (PINs)) whose disclosure or modification can compromise the security of a cryptographic module. SOURCE: FIPS 140-2
Criticality Level –	Refers to the (consequences of) incorrect behavior of a system. The more serious the expected direct and indirect effects of incorrect behavior, the higher the criticality level. SOURCE: SP 800-60
Cross-Certificate –	A certificate used to establish a trust relationship between two Certification Authorities. SOURCE: SP 800-32
Cryptanalysis –	1) Operations performed in defeating cryptographic protection without an initial knowledge of the key employed in providing the protection. 2) The study of mathematical techniques for attempting to defeat cryptographic techniques and information system security. This includes the process of looking for errors or weaknesses in the implementation of an algorithm or of the algorithm itself. SOURCE: SP 800-57
Crypto Officer –	An operator or process (subject), acting on behalf of the operator, performing cryptographic initialization or management functions. SOURCE: FIPS 140-2
Cryptographic Algorithm –	A well-defined computational procedure that takes variable inputs, including a cryptographic key, and produces an output. SOURCE: SP 800-21 [2nd Ed]
Cryptographic Boundary –	An explicitly defined continuous perimeter that establishes the physical bounds of a cryptographic module and contains all the hardware, software, and/or firmware components of a cryptographic module. SOURCE: FIPS 140-2

Cryptographic 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.

SOURCE: SP 800-21 [2nd Ed]

Cryptographic Key –

A value used to control cryptographic operations, such as decryption, encryption, signature generation or signature verification.

SOURCE: SP 800-63

A parameter used in conjunction with a cryptographic algorithm that determines the specific operation of that algorithm.

SOURCE: FIPS 201; FIPS 198

A parameter used in conjunction with a cryptographic algorithm that determines
- the transformation of plaintext data into ciphertext data,
- the transformation of ciphertext data into plaintext data,
- a digital signature computed from data,
- the verification of a digital signature computed from data,
- an authentication code computed from data, or
- an exchange agreement of a shared secret.

SOURCE: FIPS 140-2

Cryptographic Module –

The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module.

SOURCE: SP 800-32; FIPS 196

The set of hardware, software, and/or firmware that implements Approved security functions (including cryptographic algorithms and key generation) and is contained within the cryptographic boundary.

SOURCE: FIPS 140-2

Cryptographic Module Security Policy –

A precise specification of the security rules under which a cryptographic module will operate, including the rules derived from the requirements of this standard (FIPS 140-2) and additional rules imposed by the vendor.

SOURCE: FIPS 140-2

Cryptographic Module Validation Program – (CMVP)	Validates cryptographic modules to Federal Information Processing Standard (FIPS) 140-2 and other cryptography based standards. The CMVP is a joint effort between National Institute of Standards and Technology (NIST) and the Communications Security Establishment (CSE) of the Government of Canada. Products validated as conforming to FIPS 140-2 are accepted by the Federal agencies of both countries for the protection of sensitive information (United States) or Designated Information (Canada). The goal of the CMVP is to promote the use of validated cryptographic modules and provide Federal agencies with a security metric to use in procuring equipment containing validated cryptographic modules. SOURCE: FIPS 140-2
Cryptographic Strength –	A measure of the expected number of operations required to defeat a cryptographic mechanism. SOURCE: SP 800-63
Cryptographic Token –	A token where the secret is a cryptographic key. SOURCE: SP 800-63
Cryptography –	The discipline that embodies the principles, means, and methods for the transformation of data in order to hide their semantic content, prevent their unauthorized use, or prevent their undetected modification. SOURCE: SP 800-59; ANSDIT The discipline that embodies principles, means and methods for providing information security, including confidentiality, data integrity, non-repudiation, and authenticity. SOURCE: SP 800-21 [2nd Ed] Is categorized as either secret key or public key. Secret key cryptography is based on the use of a single cryptographic key shared between two parties . The same key is used to encrypt and decrypt data. This key is kept secret by the two parties. Public key cryptography is a form of cryptography which make use of two keys: a public key and a private key. The two keys are related but have the property that, given the public key, it is computationally infeasible to derive the private key [FIPS 140-1]. In a public key cryptosystem, each party has its own public/private key pair. The public key can be known by anyone; the private key is kept secret. SOURCE: FIPS 191
Cryptology –	The science that deals with hidden, disguised, or encrypted communications. It includes communications security and communications intelligence. SOURCE: SP 800-60

Cryptoperiod –	Time span during which each key setting remains in effect. SOURCE: SP 800-32
CVE –	SEE Common Vulnerabilities and Exposures.
Cyclical Redundancy Check – (CRC)	A method to ensure data has not been altered after being sent through a communication channel. SOURCE: SP 800-72
DAA –	SEE Designated Approving Authority
Data Element –	A basic unit of information that has a unique meaning and subcategories (data items) of distinct value. Examples of data elements include gender, race, and geographic location. SOURCE: SP 800-47
Data Encryption Algorithm – (DEA)	The cryptographic engine that is used by the Triple Data Encryption Algorithm (TDEA). SOURCE: SP 800-67
Data Encryption Standard – (DES)	A U.S. Government-approved, symmetric cipher, encryption algorithm used by business and civilian government agencies. The Advanced Encryption Standard (AES) is designed to replace DES. The original "single" DES algorithm is no longer secure because it is now possible to try every possible key with special purpose equipment or a high performance cluster. Triple DES (see glossary entry below), however, is still considered to be secure. SOURCE: SP 800-46
Data Integrity –	The property that data has not been altered in an unauthorized manner. Data integrity covers data in storage, during processing, and while in transit. SOURCE: SP 800-27A
Decryption –	The process of transforming ciphertext into plaintext. SOURCE: SP 800-67 The process of changing ciphertext into plaintext using a cryptographic algorithm and key. SOURCE: SP 800-21 [2nd Ed] Conversion of ciphertext to plaintext through the use of a cryptographic algorithm. SOURCE: FIPS 185

Deleted File –	A file that has been logically, but not necessarily physically, erased from the operating system, perhaps to eliminate potentially incriminating evidence. Deleting files does not always necessarily eliminate the possibility of recovering all or part of the original data. SOURCE: SP 800-72
Demilitarized Zone – (DMZ)	A network created by connecting two firewalls. Systems that are externally accessible but need some protections are usually located on DMZ networks. SOURCE: SP 800-41
Denial of Service – (DoS)	The prevention of authorized access to resources or the delaying of time-critical operations. (Time-critical may be milliseconds or it may be hours, depending upon the service provided.) SOURCE: SP 800-27A
Designated Approving (Accrediting) Authority – (DAA)	The individual selected by an authorizing official to act on their behalf in coordinating and carrying out the necessary activities required during the security certification and accreditation of an information system. SOURCE: SP 800-37
Dynamic Host Configuration Protocol – (DHCP)	The protocol used to assign Internet Protocol (IP) addresses to all nodes on the network. SOURCE: SP 800-48
Differential Power Analysis – (DPA)	An analysis of the variations of the electrical power consumption of a cryptographic module, using advanced statistical methods and/or other techniques, for the purpose of extracting information correlated to cryptographic keys used in a cryptographic algorithm. SOURCE: FIPS 140-2
Digital Evidence –	Electronic information stored or transferred in digital form. SOURCE: SP 800-72
	An asymmetric key operation where the private key is used to digitally sign an electronic document and the public key is used to verify the signature. Digital signatures provide authentication and integrity protection. SOURCE: SP 800-63
	A nonforgeable transformation of data that allows the proof of the source (with nonrepudiation) and the verification of the integrity of that data. SOURCE: FIPS 196

The result of a cryptographic transformation of data which, when properly implemented, provides the services of:

1. origin authentication
2. data integrity, and
3. signer non-repudiation.

SOURCE: FIPS 140-2

Digital Signature Algorithm – Asymmetric algorithms used for digitally signing data.

SOURCE: SP 800-49

Disaster Recovery Plan – (DRP) A written plan for processing critical applications in the event of a major hardware or software failure or destruction of facilities.

SOURCE: SP 800-34

Disconnection – The termination of an interconnection between two or more IT systems. A disconnection may be planned (e.g., due to changed business needs) or unplanned (i.e., due to an attack or other contingency).

SOURCE: SP 800-47

Discretionary Access Control – The basis of this kind of security is that an individual user, or program operating on the user's behalf is allowed to specify explicitly the types of access other users (or programs executing on their behalf) may have to information under the user's control.

SOURCE: FIPS 191

Disruption – An unplanned event that causes the general system or major application to be inoperable for an unacceptable length of time (e.g., minor or extended power outage, extended unavailable network, or equipment or facility damage or destruction).

SOURCE: SP 800-34

Distinguishing Identifier – Information which unambiguously distinguishes an entity in the authentication process.

SOURCE: FIPS 196

Distributed Denial of Service – (DDoS) A Denial of Service technique that uses numerous hosts to perform the attack.

SOURCE: SP 800-61

DMZ – SEE Demilitarized Zone.

Domain – A set of subjects, their information objects, and a common security policy.

SOURCE: SP 800-27A

Dual-Use Certificate –	A certificate that is intended for use with both digital signature and data encryption services. SOURCE: SP 800-32
Due Care –	The responsibility that managers and their organizations have a duty to provide for information security to ensure that the type of control, the cost of control, and the deployment of control are appropriate for the system being managed. SOURCE: SP 800-30
Duplicate Digital Evidence –	A duplicate is an accurate digital reproduction of all data objects contained on the original physical item and associated media. SOURCE: SP 800-72
Duration –	A field within a certificate that is composed of two subfields; "date of issue" and "date of next issue". SOURCE: SP 800-32
Dynamic Host Configuration Protocol – (DHCP)	The protocol used to assign Internet Protocol (IP) addresses to all nodes on the network. SOURCE: SP 800-48
Easter Egg –	Hidden functionality within an application program, which becomes activated when an undocumented, and often convoluted, set of commands and keystrokes are entered. Easter eggs are typically used to display the credits for the development team and are intended to be non-threatening. SOURCE: SP 800-28
Education (Information Security) –	Education integrates all of the security skills and competencies of the various functional specialties into a common body of knowledge . . . and strives to produce IT security specialists and professionals capable of vision and pro-active response. SOURCE: SP 800-50
Egress Filtering –	The process of blocking outgoing packets that use obviously false Internet Protocol (IP) addresses, such as source addresses from internal networks. SOURCE: SP 800-61
Electronic Authentication – (E-authentication)	The process of establishing confidence in user identities electronically presented to an information system. SOURCE: SP 800-63

Electronic Credentials – Digital documents used in authentication that bind an identity or an attribute to a subscriber's token.

SOURCE: SP 800-63

Electronic Evidence – Information and data of investigative value that is stored on or transmitted by an electronic device.

SOURCE: SP 800-72

Electronic Key Entry – The entry of cryptographic keys into a cryptographic module using electronic methods such as a smart card or a key-loading device. (The operator of the key may have no knowledge of the value of the key being entered.)

SOURCE: FIPS 140-2

Encrypted Key – A cryptographic key that has been encrypted using an Approved security function with a key encrypting key, a PIN, or a password in order to disguise the value of the underlying plaintext key.

SOURCE: FIPS 140-2

Encrypted Network – A network on which messages are encrypted (e.g. using DES, AES, or other appropriate algorithms) to prevent reading by unauthorized parties.

SOURCE: SP 800-32

Encryption – Encryption is the conversion of data into a form, called a ciphertext, which cannot be easily understood by unauthorized people.

SOURCE: SP 800-46

Conversion of plaintext to ciphertext through the use of a cryptographic algorithm.

SOURCE: FIPS 185

The process of changing plaintext into ciphertext for the purpose of security or privacy.

SOURCE: SP 800-21 [2nd Ed]

Encryption Certificate – A certificate containing a public key that is used to encrypt electronic messages, files, documents, or data transmissions, or to establish or exchange a session key for these same purposes.

SOURCE: SP 800-32

End to End Encryption – Communications encryption in which data is encrypted when being passed through a network, but routing information remains visible.

SOURCE: SP 800-12

Entity – Either a subject (an active element that operates on information or the system state) or an object (a passive element that contains or receives information).

SOURCE: SP 800-27A

An active element in an open system.

SOURCE: FIPS 188

Any participant in an authentication exchange; such a participant may be human or nonhuman, and may take the role of a claimant and/or verifier.

SOURCE: FIPS 196

Entropy – A measure of the amount of uncertainty that an attacker faces to determine the value of a secret.

SOURCE: SP 800-63

Environment – Aggregate of external procedures, conditions, and objects affecting the development, operation, and maintenance of an information system.

SOURCE: FIPS 200; CNSSI-4009

Ephemeral Keys – Short-lived cryptographic keys that are statistically unique to each execution of a key establishment process and meets other requirements of the key type (e.g., unique to each message or session).

SOURCE: SP 800-57

Error Detection Code – A code computed from data and comprised of redundant bits of information designed to detect, but not correct, unintentional changes in the data.

SOURCE: FIPS 140-2

Escrow – Something (e.g., a document, an encryption key) that is "delivered to a third person to be given to the grantee only upon the fulfillment of a condition."

SOURCE: FIPS 185

Event – Any observable occurrence in a network or system.

SOURCE: SP 800-61

Examination – A technical review that makes the evidence visible and suitable for analysis; tests performed on the evidence to determine the presence or absence of specific data.

SOURCE: SP 800-72

Exculpatory Evidence –	Evidence that tends to decrease the likelihood of fault or guilt. SOURCE: SP 800-72
Executive Agency –	An executive department specified in 5 United States Code (U.S.C.), Sec. 101; a military department specified in 5 U.S.C., Sec. 102; an independent establishment as defined in 5 U.S.C., Sec. 104(1); and a wholly owned Government corporation fully subject to the provisions of 31 U.S.C., Chapter 91. SOURCE: SP 800-53; FIPS 200; FIPS 199; 41 U.S.C., Sec. 403
Exploit Code –	A program that allows attackers to automatically break into a system. SOURCE: SP 800-40 Ver 2
False Acceptance –	When a biometric system incorrectly identifies an individual or incorrectly verifies an impostor against a claimed identity SOURCE: FIPS 201
False Acceptance Rate –	The probability that a biometric system will incorrectly identify an individual or will fail to reject an impostor. The rate given normally assumes passive impostor attempts. SOURCE: FIPS 201
False Match Rate – (FMR)	Alternative to 'False Acceptance Rate'. Used to avoid confusion in applications that reject the claimant if their biometric data matches that of an applicant. SOURCE: FIPS 201
False Non Match Rate – (FNMR)	Alternative to 'False Rejection Rate'. Used to avoid confusion in applications that reject the claimant if their biometric data matches that of an applicant. SOURCE: FIPS 201
False Positive –	An alert that incorrectly indicates that malicious activity is occurring. SOURCE: SP 800-61
False Rejection –	When a biometric system fails to identify an applicant or fails to verify the legitimate claimed identity of an applicant. SOURCE: FIPS 201
False Rejection Rate – (FRR)	The probability that a biometric system will fail to identify an applicant, or verify the legitimate claimed identity of an applicant. SOURCE: FIPS 201
Federal Agency –	SEE Agency.

Federal Bridge Certification Authority – (FBCA)	The Federal Bridge Certification Authority consists of a collection of Public Key Infrastructure components (Certificate Authorities, Directories, Certificate Policies and Certificate Practice Statements) that are used to provide peer-to-peer interoperability among Agency Principal Certification Authorities. SOURCE: SP 800-32
Federal Bridge Certification Authority Membrane –	The Federal Bridge Certification Authority Membrane consists of a collection of Public Key Infrastructure components including a variety of Certification Authority PKI products, Databases, CA specific Directories, Border Directory, Firewalls, Routers, Randomizers, etc. SOURCE: SP 800-32
Federal Bridge Certification Authority Operational Authority –	The Federal Bridge Certification Authority Operational Authority is the organization selected by the Federal Public Key Infrastructure Policy Authority to be responsible for operating the Federal Bridge Certification Authority. SOURCE: SP 800-32
Federal Information Processing Standard – (FIPS)	A standard for adoption and use by Federal agencies that has been developed within the Information Technology Laboratory and published by the National Institute of Standards and Technology, a part of the U.S. Department of Commerce. A FIPS covers some topic in information technology in order to achieve a common level of quality or some level of interoperability. SOURCE: FIPS 201
Federal Information System –	An information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency. SOURCE: SP 800-53; FIPS 200; FIPS 199; 40 U.S.C., Sec. 11331
Federal Information Systems Security Educators' Association – (FISSEA)	An organization whose members come from federal agencies, industry, and academic institutions devoted to improving the IT security awareness and knowledge within the federal government and its related external workforce. SOURCE: SP 800-16
Federal Public Key Infrastructure Policy Authority – (FPKI PA)	The Federal PKI Policy Authority is a federal government body responsible for setting, implementing, and administering policy decisions regarding interagency PKI interoperability that uses the FBCA. SOURCE: SP 800-32

File Infector Virus – A virus that attaches itself to a program file, such as a word processor, spreadsheet application, or game.

SOURCE: SP 800-61

File Integrity Checker – Software that generates, stores, and compares message digests for files to detect changes to the files.

SOURCE: SP 800-61

File Name Anomaly –

1) A mismatch between the internal file header and its external extension;
2) A file name inconsistent with the content of the file (e.g., renaming a graphics file with a non-graphical extension.

SOURCE: SP 800-72

FIPS – SEE Federal Information Processing Standard

FIPS Approved Security Method – A security method (e.g., cryptographic algorithm, cryptographic key generation algorithm or key distribution technique, random number generator, authentication technique, or evaluation criteria) that is either a) specified in a FIPS, or b) adopted in a FIPS.

SOURCE: FIPS 196

FIPS PUB – An acronym for Federal Information Processing Standards Publication. FIPS publications (PUB) are issued by NIST after approval by the Secretary of Commerce.

SOURCE: SP 800-64

Firewall – A gateway that limits access between networks in accordance with local security policy.

SOURCE: SP 800-32

Firewall Control Proxy – The component that controls a firewall's handling of a call. The firewall control proxy can instruct the firewall to open specific ports that are needed by a call, and direct the firewall to close these ports at call termination.

SOURCE: SP 800-58

Firewall Environment – A firewall environment is a collection of systems at a point on a network that together constitute a firewall implementation. A firewall environment could consist of one device or many devices such as several firewalls, intrusion detection systems, and proxy servers.

SOURCE: SP 800-41

Firewall Platform – A firewall platform is the system device upon which a firewall is implemented. An example of a firewall platform is a commercial operating system running on a personal computer.

SOURCE: SP 800-41

Firewall Ruleset – A firewall ruleset is a table of instructions that the firewall uses for determining how packets should be routed between its interfaces. In routers, the ruleset can be a file that the router examines from top to bottom when making routing decisions.

SOURCE: SP 800-41

Firmware – The programs and data components of a cryptographic module that are stored in hardware within the cryptographic boundary and cannot be dynamically written or modified during execution.

SOURCE: FIPS 140-2

FISMA – Federal Information Security Management Act - requires agencies to integrate IT security into their capital planning and enterprise architecture processes at the agency, conduct annual IT security reviews of all programs and systems, and report the results of those reviews to the Office of Management and Budget (OMB).

SOURCE: SP 800-65

Forensic Copy – An accurate bit-for-bit reproduction of the information contained on an electronic device or associated media, whose validity and integrity has been verified using an accepted algorithm.

SOURCE: SP 800-72

Forensic Specialist – A professional who locates, identifies, collects, analyzes and examines data while preserving the integrity and maintaining a strict chain of custody of information discovered.

SOURCE: SP 800-72

Forensics, Computer – The practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data.

SOURCE: SP 800-61

Formatting Function – The function that transforms the payload, associated data, and nonce into a sequence of complete blocks.

SOURCE: SP 800-38C

Forward Cipher – One of the two functions of the block cipher algorithm that is determined by the choice of a cryptographic key.

SOURCE: SP 800-67

General Support System –

An interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, and people.

SOURCE: SP 800-53; OMB Circular A-130, App. III

Graduated Security –

A security system that provides several levels (e.g., low, moderate, high) of protection based on threats, risks, available technology, support services, time, human concerns, and economics.

SOURCE: FIPS 201

Guard (System) –

A mechanism limiting the exchange of information between information systems or subsystems.

SOURCE: SP 800-53 Rev 1; CNSSI-4009 Adapted

Guessing Entropy –

A measure of the difficulty that an attacker has 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.

SOURCE: SP 800-63

Handler –

A type of program used in DDoS attacks to control agents distributed throughout a network. Also refers to an incident handler, which refers to a person who performs incident response work.

SOURCE: SP 800-61

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 that maps to any pre-specified output.
2) Collision Resistant. It is computationally infeasible to find any two distinct inputs that map to the same output.

SOURCE: SP 800-63; FIPS 201

An Approved mathematical function that maps a string of arbitrary length (up to a pre-determined maximum size) to a fixed length string. It may be used to produce a checksum, called a hash value or message digest, for a potentially long string or message.

SOURCE: FIPS 198

Hash-based Message Authentication Code –
(HMAC)

A symmetric key authentication method using hash functions.

SOURCE: SP 800-63

A message authentication code that uses a cryptographic key in conjunction with a hash function.

SOURCE: FIPS 201

A message authentication code that utilizes a keyed hash.

SOURCE: FIPS 140-2

Hashing – The process of using a mathematical algorithm against data to produce a numeric value that is representative of that data.

SOURCE: SP 800-72

High Assurance Guard – (HAG) An enclave boundary protection device that controls access between a local area network that an enterprise system has a requirement to protect, and an external network that is outside the control of the enterprise system, with a high degree of assurance.

SOURCE: SP 800-32

High Impact System – An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of high.

SOURCE: SP 800-53; FIPS 200

Honeypot – A host that is designed to collect data on suspicious activity and has no authorized users other than its administrators.

SOURCE: SP 800-61

Hot Site – A fully operational off-site data processing facility equipped with hardware and system software to be used in the event of a disaster.

SOURCE: SP 800-34

Identification – The process of verifying the identity of a user, process, or device, usually as a prerequisite for granting access to resources in an IT system.

SOURCE: SP 800-47

The process of discovering the true identity (i.e., origin, initial history) of a person or item from the entire collection of similar persons or items.

SOURCE: FIPS 201

Identifier – A unique data string used as a key in the biometric system to name a person's identity and its associated attributes.

SOURCE: FIPS 201

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 to make the complete name unique.

SOURCE: SP 800-63

The set of physical and behavioral characteristics by which an individual is uniquely recognizable.

SOURCE: FIPS 201

Identity-Based Security Policy – A security policy based on the identities and/or attributes of the object (system resource) being accessed and of the subject (user, group of users, process, or device) requesting access.

SOURCE: SP 800-33

Identity Binding – Binding of the vetted claimed identity to the individual (through biometrics) according to the issuing authority.

SOURCE: FIPS 201

Identity Proofing – The process by which a Credentials Service Provider (CSP) and a Registration Authority (RA) validate sufficient information to uniquely identify a person.

SOURCE: SP 800-63

The process of providing sufficient information (e.g., identity history, credentials, documents) to a Personal Identity Verification Registrar when attempting to establish an identity.

SOURCE: FIPS 201

Identity Registration – The process of making a person's identity known to the Personal Identity Verification (PIV) system, associating a unique identifier with that identity, and collecting and recording the person's relevant attributes into the system.

SOURCE: FIPS 201

Identity Verification – The process of affirming that a claimed identity is correct by comparing the offered claims of identity with previously proven information stored in the identity card or PIV system.

SOURCE: FIPS 201

The process of confirming or denying that a claimed identity is correct by comparing the credentials (something you know, something you have, something you are) of a person requesting access with those previously proven and stored in the PIV Card or system and associated with the identity being claimed.

SOURCE: SP 800-79

IDS – SEE Intrusion Detection System

IDS – Host-Based – IDSs which operate on information collected from within an individual computer system. This vantage point allows host-based IDSs to determine exactly which processes and user accounts are involved in a particular attack on the Operating System. Furthermore, unlike network-based IDSs, host-based IDSs can more readily "see" the intended outcome of an attempted attack, because they can directly access and monitor the data files and system processes usually targeted by attacks.

SOURCE: SP 800-36

IDS – Network-Based – IDSs which detect attacks by capturing and analyzing network packets. Listening on a network segment or switch, one network-based IDS can monitor the network traffic affecting multiple hosts that are connected to the network segment.

SOURCE: SP 800-36

Image – An exact bit-stream copy of all electronic data on a device, performed in a manner that ensures the information is not altered.

SOURCE: SP 800-72

Impact – The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability.

SOURCE: SP 800-60

Inappropriate Usage – A person who violates acceptable computing use policies.

SOURCE: SP 800-61

Incident – A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices.

SOURCE: SP 800-61

An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

SOURCE: FIPS 200

Incident Handling – The mitigation of violations of security policies and recommended practices.

SOURCE: SP 800-61

Incident Response Plan – The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyber attacks against an organization's IT systems(s).

SOURCE: SP 800-34

Inculpatory Evidence – Evidence that tends to increase the likelihood of fault or guilt.

SOURCE: SP 800-72

Indication – A sign that an incident may have occurred or may be currently occurring.

SOURCE: SP 800-61

Individual – A citizen of the United States or an alien lawfully admitted for permanent residence. Agencies may, consistent with individual practice, choose to extend the protections of the Privacy Act and E-Government Act to businesses, sole proprietors, aliens, etc.

SOURCE: SP 800-60

Information – An instance of an information type.

SOURCE: FIPS 200

Information Assurance – Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

SOURCE: SP 800-59; CNSSI-4009

Information Owner – Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.

SOURCE: SP 800-53; CNSSI-4009

Information Resources – Information and related resources, such as personnel, equipment, funds, and information technology.

SOURCE: SP 800-53; 44 U.S.C., Sec. 3502

Information and related resources, such as personnel, equipment, funds, and information technology.

SOURCE: FIPS 200; FIPS 199

Information Security – The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

SOURCE: SP 800-53; FIPS 200; FIPS 199; 44 U.S.C., Sec. 3542

Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—

1) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;
2) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and
3) availability, which means ensuring timely and reliable access to and use of information.

SOURCE: SP 800-66; 44 U.S.C., Sec 3541

Information Security Policy – Aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information.

SOURCE: SP 800-53; CNSSI-4009

Information Sharing – The requirements for information sharing by an IT system with one or more other IT systems or applications, for information sharing to support multiple internal or external organizations, missions, or public programs.

SOURCE: SP 800-16

Information System – A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

SOURCE: SP 800-53; FIPS 200; FIPS 199; 44 U.S.C., Sec. 3502; OMB Circular A-130, App. III

Information System Owner (or Program Manager) – Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.

SOURCE: SP 800-53; CNSSI-4009 Adapted

Information System Owner – Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.

SOURCE: FIPS 200; CNSSI-4009 Adapted

Information System Security Officer – (ISSO)	Individual assigned responsibility by the senior agency information security officer, authorizing official, management official, or information system owner for ensuring the appropriate operational security posture is maintained for an information system or program. SOURCE: SP 800-53; CNSSI-4009 Adapted
Information Technology –	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which— 1) requires the use of such equipment; or 2) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. SOURCE: SP 800-53; FIPS 200; FIPS 199; 40 U.S.C., Sec. 11101
Information Type –	A specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management), defined by an organization or in some instances, by a specific law, executive order, directive, policy, or regulation. SOURCE: SP 800-53; FIPS 200; FIPS 199
Ingress Filtering –	The process of blocking incoming packets that use obviously false IP addresses, such as reserved source addresses. SOURCE: SP 800-61
Initialization Vector – (IV)	A vector used in defining the starting point of an encryption process within a cryptographic algorithm. SOURCE: SP 800-57; FIPS 140-2
Initiator –	The entity that initiates an authentication exchange. SOURCE: FIPS 196
Inside Threat –	An entity with authorized access that has the potential to harm an information system through destruction, disclosure, modification of data, and/or denial of service. SOURCE: SP 800-32

Integrity –	Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. SOURCE: SP 800-53; FIPS 200; FIPS 199; 44 U.S.C., Sec. 3542 The property that sensitive data has not been modified or deleted in an unauthorized and undetected manner. SOURCE: FIPS 140-2
Intellectual Property –	Useful artistic, technical, and/or industrial information, knowledge or ideas that convey ownership and control of tangible or virtual usage and/or representation. SOURCE: SP 800-32
Interconnection, System –	SEE System Interconnection
Interconnection Security Agreement – (ISA)	An agreement established between the organizations that own and operate connected IT systems to document the technical requirements of the interconnection. The ISA also supports a Memorandum of Understanding or Agreement (MOU/A) between the organizations. SOURCE: SP 800-47
Intermediate Certification Authority – (CA)	A Certification Authority that is subordinate to another CA, and has a CA subordinate to itself. SOURCE: SP 800-32
Interoperability –	In FIPS 201, interoperability allows any Government facility or information system, regardless of the cardholder's parent organization, to authenticate cardholder's identity using the credentials stored on the Personal Identity Verification (PIV) card. SOURCE: FIPS 201
Intrusion Detection System – (IDS)	Software that looks for suspicious activity and alerts administrators. SOURCE: SP 800-61
Intrusion Prevention Systems –	Systems which can detect an intrusive activity and can also attempt to stop the activity, ideally before it reaches its targets. SOURCE: SP 800-36
Inverse Cipher –	Series of transformations that converts ciphertext to plaintext using the Cipher Key. SOURCE: FIPS 197

IP Address –

An IP address is a unique number for a computer that is used to determine where messages transmitted on the Internet should be delivered. The IP address is analogous to a house number for ordinary postal mail.

SOURCE: SP 800-46

IP Security – (IPsec)

An Institute of Electrical and Electronic Engineers (IEEE) standard, Request For Comments (RFC) 2411, protocol that provides security capabilities at the Internet Protocol (IP) layer of communications. IPsec's key management protocol is used to negotiate the secret keys that protect Virtual Private Network (VPN) communications, and the level and type of security protections that will characterize the VPN. The most widely used key management protocol is the Internet Key Exchange (IKE) protocol.

SOURCE: SP 800-46

IT-Related Risk –

The net mission/business impact considering

1) the likelihood that a particular threat source will exploit, or trigger, a particular information system vulnerability, and
2) the resulting impact if this should occur. IT-related risks arise from legal liability or mission/business loss due to, but not limited to:
   - Unauthorized (malicious, non-malicious, or accidental) disclosure, modification, or destruction of information.
   - Non-malicious errors and omissions.
   - IT disruptions due to natural or man-made disasters.
   - Failure to exercise due care and diligence in the implementation and operation of the IT.

SOURCE: SP 800-27A

IT Security Architecture –

A description of security principles and an overall approach for complying with the principles that drive the system design; i.e., guidelines on the placement and implementation of specific security services within various distributed computing environments.

SOURCE: SP 800-27A

IT Security Awareness –

The purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly.

SOURCE: SP 800-50

IT Security Awareness and Training Program –

Explains proper rules of behavior for the use of agency IT systems and information. The program communicates IT security policies and procedures that need to be followed.

SOURCE: SP 800-50

IT Security Education – IT Security Education seeks to integrate all of the security skills and competencies of the various functional specialties into a common body of knowledge, adds a multidisciplinary study of concepts, issues, and principles (technological and social), and strives to produce IT security specialists and professionals capable of vision and pro-active response.

SOURCE: SP 800-50

IT Security Goal – The five security goals are confidentiality, availability, integrity, accountability, and assurance.

SOURCE: SP 800-27A

IT Security Investment – An IT application or system that is solely devoted to security. For instance, intrusion detection systems (IDS) and public key infrastructure (PKI) are examples of IT security investments.

SOURCE: SP 800-65

IT Security Metrics – Metrics based on IT security performance goals and objectives.

SOURCE: SP 800-55

IT Security Policy – The "documentation of IT security decisions" in an organization.

NIST SP 800-12 categorizes IT Security Policy into three basic types:

1) Program Policy—high-level policy used to create an organization's IT security program, define its' scope within the organization, assign implementation responsibilities, establish strategic direction, and assign resources for implementation.
2) Issue-Specific Policies—address specific issues of concern to the organization, such as contingency planning, the use of a particular methodology for systems risk management, and implementation of new regulations or law. These policies are likely to require more frequent revision as changes in technology and related factors take place.
3) System-Specific Policies—address individual systems, such as establishing an access control list or in training users as to what system actions are permitted. These policies may vary from system to system within the same organization. In addition, policy may refer to entirely different matters, such as the specific managerial decisions setting an organization's electronic mail (e-mail) policy or fax security policy.

SOURCE: SP 800-35

IT Security Training –

IT Security Training strives to produce relevant and needed security skills and competencies by practitioners of functional specialties other than IT security (e.g., management, systems design and development, acquisition, auditing). The most significant difference between training and awareness is that training seeks to teach skills, which allow a person to perform a specific function, while awareness seeks to focus an individual's attention on an issue or set of issues. The skills acquired during training are built upon the awareness foundation, in particular, upon the security basics and literacy material.

SOURCE: SP 800-50

Kerberos –

A widely used authentication protocol developed at the Massachusetts Institute of Technology (MIT). In "classic" Kerberos, users share a secret password with a Key Distribution Center (KDC). The user, Alice, who wishes to communicate with another user, Bob, authenticates to the KDC and is furnished a "ticket" by the KDC to use to authenticate with Bob. When Kerberos authentication is based on passwords, the protocol is known to be vulnerable to off-line dictionary attacks by eavesdroppers who capture the initial user-to-KDC exchange.

SOURCE: SP 800-63

Key –

A value used to control cryptographic operations, such as decryption, encryption, signature generation or signature verification.

SOURCE: SP 800-63

Key Bundle –

The three cryptographic keys (Key1, Key2, Key3) that are used with a Triple Data Encryption Algorithm mode.

SOURCE: SP 800-67

Key Escrow –

A deposit of the private key of a subscriber and other pertinent information pursuant to an escrow agreement or similar contract binding upon the subscriber, the terms of which require one or more agents to hold the subscriber's private key for the benefit of the subscriber, an employer, or other party, upon provisions set forth in the agreement.

SOURCE: SP 800-32

The processes of managing (e.g., generating, storing, transferring, auditing) the two components of a cryptographic key by two key component holders.

SOURCE: FIPS 185

Key Escrow System – A system that entrusts the two components comprising a cryptographic key (e.g., a device unique key) to two key component holders (also called "escrow agents").

SOURCE: FIPS 185

Key Establishment – The process by which cryptographic keys are securely distributed among cryptographic modules using manual transport methods (e.g., key loaders), automated methods (e.g., key transport and/or key agreement protocols), or a combination of automated and manual methods (consists of key transport plus key agreement).

SOURCE: FIPS 140-2

Key Exchange – The process of exchanging public keys in order to establish secure communications.

SOURCE: SP 800-32; CNSSI-4009 Adapted

Key Expansion – Routine used to generate a series of Round Keys from the Cipher Key.

SOURCE: FIPS 197

Key Generation Material – Random numbers, pseudo-random numbers, and cryptographic parameters used in generating cryptographic keys.

SOURCE: SP 800-32

Key Loader – A self-contained unit that is capable of storing at least one plaintext or encrypted cryptographic key or key component that can be transferred, upon request, into a cryptographic module.

SOURCE: FIPS 140-2

Key Management – The activities involving the handling of cryptographic keys and other related security parameters (e.g., IVs and passwords) during the entire life cycle of the keys, including their generation, storage, establishment, entry and output, and zeroization.

SOURCE: FIPS 140-2

Key Pair – Two mathematically related keys having the properties that (1) one key can be used to encrypt a message that can only be decrypted using the other key, and 2) even knowing one key, it is computationally infeasible to discover the other key.

SOURCE: SP 800-32

A public key and its corresponding private key; a key pair is used with a public key algorithm.

SOURCE: SP 800-21 [2nd Ed]; CNSSI-4009 Adapted

Key Transport –	The secure transport of cryptographic keys from one cryptographic module to another module. SOURCE: FIPS 140-2
Key Wrap –	A method of encrypting keys (along with associated integrity information) that provides both confidentiality and integrity protection using a symmetric key algorithm. SOURCE: SP 800-56
Keyed-hash based message authentication code – (HMAC)	A message authentication code that uses a cryptographic key in conjunction with a hash function. SOURCE: FIPS 198
Keystroke Monitoring –	The process used to view or record both the keystrokes entered by a computer user and the computer's response during an interactive session. Keystroke monitoring is usually considered a special case of audit trails. SOURCE: SP 800-12
Label –	SEE Security Label.
Least Privilege –	The security objective of granting users only those accesses they need to perform their official duties. SOURCE: SP 800-12
Link Encryption –	Link encryption encrypts all of the data along a communications path (e.g., a satellite link, telephone circuit, or T1 line). Since link encryption also encrypts routing data, communications nodes need to decrypt the data to continue routing. SOURCE: SP 800-12
Local Registration Authority – (LRA)	A Registration Authority with responsibility for a local community. SOURCE: SP 800-32
Low Impact System –	An information system in which all three security objectives (i.e., confidentiality, integrity, and availability) are assigned a FIPS 199 potential impact of low. SOURCE: SP 800-53; FIPS 200
Macro Virus –	A virus that attaches itself to documents and uses the macro programming capabilities of the document's application to execute and propagate. SOURCE: SP 800-61

Major Application –	An application that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Note: All federal applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight and should be treated as major. Adequate security for other applications should be provided by security of the systems in which they operate. SOURCE: SP 800-53; OMB Circular A-130, App. III
Major Information System –	An information system that requires special management attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs, finances, property, or other resources. SOURCE: SP 800-53; OMB Circular A-130, App. III
Malicious Code –	Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. SOURCE: SP 800-53 Rev 1; CNSSI-4009
Malware –	A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim. SOURCE: SP 800-83
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. SOURCE: SP 800-63
Management Controls –	The security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information system security. SOURCE: SP 800-53; FIPS 200
Mandatory Access Control –	A means of restricting access to system resources based on the sensitivity (as represented by a label) of the information contained in the system resource and the formal authorization (i.e., clearance) of users to access information of such sensitivity. SOURCE: SP 800-44; CNSSI-4009 Adapted

	Access controls (which) are driven by the results of a comparison between the user's trust level or clearance and the sensitivity designation of the information. SOURCE: FIPS 191
Mandatory Topography –	The format and information required to be displayed on a PIV card. Also known as the Standard Topography. SOURCE: FIPS 201
Manual Key Transport –	A non-electronic means of transporting cryptographic keys by physically moving a device, document or person containing or possessing the key or a key component. SOURCE: SP 800-57 A non-electronic means of transporting cryptographic keys. SOURCE: FIPS 140-2
Masquerading –	When an unauthorized agent claims the identity of another agent it is said to be masquerading. SOURCE: SP 800-19
Match/matching –	The process of comparing biometric information against a previously stored template(s) and scoring the level of similarity. SOURCE: FIPS 201
Media –	Physical devices or writing surfaces including but not limited to magnetic tapes, optical disks, magnetic disks, LSI memory chips, printouts (but not including display media) onto which information is recorded, stored, or printed within an information system. SOURCE: FIPS 200
Media Sanitization –	A general term referring to the actions taken to render data written on media unrecoverable by both ordinary and extraordinary means. SOURCE: SP 800-88
Memorandum of Understanding/Agreement – (MOU/A)	A document established between two or more parties to define their respective responsibilities in accomplishing a particular goal or mission. In this guide, an MOU/A defines the responsibilities of two or more organizations in establishing, operating, and securing a system interconnection. SOURCE: SP 800-47
Message Authentication Code – (MAC)	A cryptographic checksum on data that uses a symmetric key to detect both accidental and intentional modifications of the data. SOURCE: SP 800-63; FIPS 201

A cryptographic checksum that results from passing data through a message authentication algorithm.

SOURCE: FIPS 198

Message Digest – A cryptographic checksum, typically generated for a file that can be used to detect changes to the file; Secure Hash Algorithm-1 (SHA-1) is an example of a message digest algorithm

SOURCE: SP 800-61

Metrics – Tools designed to facilitate decision-making and improve performance and accountability through collection, analysis, and reporting of relevant performance-related data.

SOURCE: SP 800-55

MIME – SEE Multipurpose Internet Mail Extensions.

Min-Entropy – A measure of the difficulty that an attacker has to guess the most commonly chosen password used in a system.

SOURCE: SP 800-63

Minor Application – An application, other than a major application, that requires attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Minor applications are typically included as part of a general support system.

SOURCE: SP 800-53

Misnamed Files – A technique used to disguise a file's content by changing the file's name to something innocuous or altering its extension to a different type of file, forcing the examiner to identify the files by file signature versus file extension.

SOURCE: SP 800-72

Mission Critical – Any telecommunications or information system that is defined as a national security system (Federal Information Security Management Act of 2002 - FISMA) or processes any information the loss, misuse, disclosure, or unauthorized access to or modification of, would have a debilitating impact on the mission of an agency.

SOURCE: SP 800-60

Mobile Code – Software programs or parts of programs obtained from remote information systems, transmitted across a network, and executed on a local information system without explicit installation or execution by the recipient.

SOURCE: SP 800-53; CNSSI-4009 Adapted

Mobile Code Technologies –	Software technologies that provide the mechanisms for the production and use of mobile code (e.g., Java, JavaScript, ActiveX, VBScript). SOURCE: SP 800-53
Mobile Site –	A self-contained, transportable shell custom-fitted with the specific IT equipment and telecommunications necessary to provide full recovery capabilities upon notice of a significant disruption. SOURCE: SP 800-34
Mobile Software Agent –	Programs that are goal-directed and capable of suspending their execution on one platform and moving to another platform where they resume execution. SOURCE: SP 800-19
Mode of Operation –	An algorithm for the cryptographic transformation of data that features a symmetric key block cipher algorithm. SOURCE: SP 800-38C
Moderate Impact System –	An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of moderate and no security objective is assigned a FIPS 199 potential impact value of high. SOURCE: SP 800-53; FIPS 200
Multi-Hop Problem –	The security risks resulting from a mobile software agent visiting several platforms. SOURCE: SP 800-19
Multiple Component Incident –	A single incident that encompasses two or more incidents. SOURCE: SP 800-61
Multipurpose Internet Mail Extensions – (MIME)	An extensible mechanism for email. A variety of MIME types exist for sending content such as audio using the Simple Mail Transfer Protocol (SMTP) protocol. SOURCE: SP 800-41
Mutual Authentication –	Occurs when parties at both ends of a communication activity authenticate each other. SOURCE: SP 800-32
Naming Authority –	An organizational entity responsible for assigning distinguished names (DNs) and for assuring that each DN is meaningful and unique within its domain. SOURCE: SP 800-32

National Security Emergency Preparedness Telecommunications Services –

Telecommunications services that are used to maintain a state of readiness or to respond to and manage any event or crisis (local, national, or international) that causes or could cause injury or harm to the population, damage to or loss of property, or degrade or threaten the national security or emergency preparedness posture of the United States.

SOURCE: SP 800-53; 47 C.F.R., Part 64, App A

Needs Assessment (IT Security Awareness and Training) –

A process that can be used to determine an organization's awareness and training needs. The results of a needs assessment can provide justification to convince management to allocate adequate resources to meet the identified awareness and training needs.

SOURCE: SP 800-50

National Information Assurance Partnership –
(NIAP)

A U.S. Government initiative originated to meet the security testing needs of both information technology (IT) consumers and producers. NIAP is a collaboration between the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) in fulfilling their respective responsibilities under Public Law (PL) 100-235 (Computer Security Act of 1987). The partnership combines the extensive IT security experience of both agencies to promote the development of technically sound security requirements for IT products and systems and appropriate measures for evaluating those products and systems.

SOURCE: SP 800-64

Non-repudiation –

Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information.

SOURCE: SP 800-53; CNSSI-4009

Is the security service by which the entities involved in a communication cannot deny having participated. Specifically the sending entity cannot deny having sent a message (non-repudiation with proof of origin) and the receiving entity cannot deny having received a message (non-repudiation with proof of delivery).

SOURCE: FIPS 191

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 than a random challenge, because a nonce is not necessarily unpredictable.

SOURCE: SP 800-63

Object –	A passive entity that contains or receives information. SOURCE: SP 800-27A; CNSSI-4009 Adapted
Object Identifier –	A specialized formatted number that is registered with an internationally recognized standards organization. The unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class. In the federal government PKI they are used to uniquely identify each of the four policies and cryptographic algorithms supported. SOURCE: SP 800-32
Off-Card –	Refers to data that is not stored within the PIV card or computation that is not done by the Integrated Circuit Chip (ICC) of the PIV card. SOURCE: FIPS 201
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 he/she is able to analyze in a system of his/her own choosing. SOURCE: SP 800-63
On-Card –	Refers to data that is stored within the PIV card or computation that is done by the ICC of the PIV card. SOURCE: FIPS 201
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. SOURCE: SP 800-63
On-Line Certificate Status Protocol – (OCSP)	An on-line protocol used to determine the status of a public key certificate. SOURCE: SP 800-63
One-Way Hash Algorithm –	Hash algorithms which map arbitrarily long inputs into a fixed-size output such that it is very difficult (computationally infeasible) to find two different hash inputs that produce the same output. Such algorithms are an essential part of the process of producing fixed-size digital signatures that can both authenticate the signer and provide for data integrity checking (detection of input modification after signature). SOURCE: SP 800-49

Online Certification Status Protocol – (OCSP)	An on-line protocol used to determine the status of a public key certificate. SOURCE: FIPS 201
Operational Controls –	The security controls (i.e., safeguards or countermeasures) for an information system that primarily are implemented and executed by people (as opposed to systems). SOURCE: SP 800-53; FIPS 200
Optional Topography –	A Personal Identity Verification (PIV) card having both the Standard Topography (Mandatory Topography) features and the Optional features as defined in FIPS 201 sections 4.1.4.3 and 4.1.4.4. SOURCE: FIPS 201
Outside Threat –	An unauthorized entity from outside the domain perimeter that has the potential to harm an Information System through destruction, disclosure, modification of data, and/or denial of service. SOURCE: SP 800-32
Packet Sniffer –	Software that observes and records network traffic. SOURCE: SP 800-61
Parent Organization –	The organization that is applying for the Personal Identity Verification card on behalf of an applicant. Typically this is an organization for whom the applicant is working. SOURCE: FIPS 201
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). SOURCE: SP 800-63
Password –	A secret that a claimant memorizes and uses to authenticate his or her identity. Passwords are typically character strings. SOURCE: SP 800-63 A protected character string used to authenticate the identity of a computer system user or to authorize access to system resources. SOURCE: FIPS 181 A string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization. SOURCE: FIPS 140-2

Password Protected –	The ability to protect a file using a password access control, protecting the data contents from being viewed with the appropriate viewer unless the proper password is entered. SOURCE: SP 800-72
Path Histories –	Maintaining an authenticatable record of the prior platforms visited by a mobile software agent, so that a newly visited platform can determine whether to process the agent and what resource constraints to apply. SOURCE: SP 800-19
Payload –	The input data to the CCM generation-encryption process that is both authenticated and encrypted. SOURCE: SP 800-38C
Personal Identification Number – (PIN)	A password consisting only of decimal digits. SOURCE: SP 800-63 A secret that a claimant memorizes and uses to authenticate his or her identity. PINS are generally only decimal digits. SOURCE: FIPS 201 An alphanumeric code or password used to authenticate an identity. SOURCE: FIPS 140-2
Personal Identity Verification Authorizing Official –	An individual who can act on behalf of an agency to authorize the issuance of a credential to an applicant. SOURCE: FIPS 201
Personal Identity Verification Card – (PIV Card)	Physical artifact (e.g., identity card, "smart" card) issued to an individual that contains stored identity credentials (e.g., photograph, cryptographic keys, digitized fingerprint representation etc.) such that a claimed identity of the cardholder may be verified against the stored credentials by another person (human readable and verifiable) or an automated process (computer readable and verifiable). SOURCE: FIPS 201
Personal Identity Verification Issuance Authority –	An authorized identity card creator that procures FIPS approved blank identity cards, initializes them with appropriate software and data elements for the requested identity verification and access control application, personalizes the card with the identity credentials of the authorized subject, and delivers the personalized card to the authorized subject along with appropriate instructions for protection and use. SOURCE: FIPS 201

Personal Identity Verification Registration Authority –

An entity that establishes and vouches for the identity of an applicant to a PIV Issuing Authority. The PIV RA authenticates the applicant's identity by checking identity source documents and identity proofing and ensures a proper background check has been completed before the credential is issued.

SOURCE: FIPS 201

Personal Identity Verification Requesting Official –

An individual who can act on behalf of an agency to request a credential for an applicant.

SOURCE: FIPS 201

Phishing –

Tricking individuals into disclosing sensitive personal information through deceptive computer-based means.

SOURCE: SP 800-83

Physically Isolated Network –

A network that is not connected to entities or systems outside a physically controlled space.

SOURCE: SP 800-32

Plaintext –

Data input to the Cipher or output from the Inverse Cipher.

SOURCE: FIPS 197

Intelligible data that has meaning and can be understood without the application of decryption.

SOURCE: SP 800-21 [2nd Ed]

Plaintext Key –

An unencrypted cryptographic key.

SOURCE: FIPS 140-2

Plan of Action and Milestones (POA&M) –

A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.

SOURCE: SP 800-53; OMB Memorandum 02-01

Policy –

A document that delineates the security management structure and clearly assigns security responsibilities and lays the foundation necessary to reliably measure progress and compliance.

ALSO SEE Security Policy.

SOURCE: SP 800-26

Policy Management Authority – (PMA)	Body established to oversee the creation and update of Certificate Policies, review Certification Practice Statements, review the results of CA audits for policy compliance, evaluate non-domain policies for acceptance within the domain, and generally oversee and manage the PKI certificate policies. For the FBCA, the PMA is the Federal PKI Policy Authority. SOURCE: SP 800-32
Policy Mapping –	Recognizing that, when a CA in one domain certifies a CA in another domain, a particular certificate policy in the second domain may be considered by the authority of the first domain to be equivalent (but not necessarily identical in all respects) to a particular certificate policy in the first domain. SOURCE: SP 800-15
Port –	A physical entry or exit point of a cryptographic module that provides access to the module for physical signals, represented by logical information flows (physically separated ports do not share the same physical pin or wire). SOURCE: FIPS 140-2
Port Scanning –	Using a program to remotely determine which ports on a system are open (e.g., whether systems allow connections through those ports). SOURCE: SP 800-61
Potential Impact –	The loss of confidentiality, integrity, or availability could be expected to have: 1) a *limited* adverse effect (FIPS 199 low); 2) a *serious* adverse effect (FIPS 199 moderate); or 3) a *severe* or *catastrophic* adverse effect (FIPS 199 high) on organizational operations, organizational assets, or individuals. SOURCE: SP 800-53 The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect; a serious adverse effect, or a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. SOURCE: FIPS 200
Practice Statement –	A formal statement of the practices followed by an authentication entity (e.g., RA, CSP, or verifier); typically the specific steps taken to register and verify identities, issue credentials and authenticate claimants. SOURCE: SP 800-63

Precursor – A sign that an attacker may be preparing to cause an incident.

SOURCE: SP 800-61

Principal – An entity whose identity can be authenticated.

SOURCE: FIPS 196

Principal Certification Authority – (CA) The Principal Certification Authority is a CA designated by an Agency to interoperate with the FBCA. An Agency may designate multiple Principal CAs to interoperate with the FBCA.

SOURCE: SP 800-32

Privacy – Restricting access to subscriber or Relying Party information in accordance with Federal law and Agency policy.

SOURCE: SP 800-32

Privacy Impact Assessment – An analysis of how information is handled: 1) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; 2) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system; and 3) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

SOURCE: SP 800-53; OMB Memorandum 03-22

Private Key – The secret part of an asymmetric key pair that is typically used to digitally sign or decrypt data.

SOURCE: SP 800-63

A cryptographic key, used with a public key cryptographic algorithm, that is uniquely associated with an entity and is not made public. In an asymmetric (public) cryptosystem, the private key is associated with a public key. Depending on the algorithm, the private key may be used to—

1) Compute the corresponding public key,
2) Compute a digital signature that may be verified by the corresponding public key,
3) Decrypt data that was encrypted by the corresponding public key, or
4) Compute a piece of common shared data, together with other information.

SOURCE: SP 800-57

	A cryptographic key used with a public key cryptographic algorithm, which is uniquely associated with an entity, and not made public; it is used to generate a digital signature; this key is mathematically linked with a corresponding public key. SOURCE: FIPS 196
	A cryptographic key, used with a public key cryptographic algorithm, that is uniquely associated with an entity and is not made public. SOURCE: FIPS 140-2
Privileged Accounts –	Individuals who have access to set "access rights" for users on a given system. Sometimes referred to as system or network administrative accounts. SOURCE: SP 800-12
Profiling –	Measuring the characteristics of expected activity so that changes to it can be more easily identified. SOURCE: SP 800-61
Proof of Possession Protocol – (PoP Protocol)	A protocol where a claimant proves to a verifier that he/she possesses and controls a token (e.g., a key or password). SOURCE: SP 800-63
Protective Distribution System –	Wire line or fiber optic system that includes adequate safeguards and/or countermeasures (e.g., acoustic, electric, electromagnetic, and physical) to permit its use for the transmission of unencrypted information. SOURCE: SP 800-53
Protocol Data Unit –	A unit of data specified in a protocol and consisting of protocol information and, possibly, user data. SOURCE: FIPS 188
Protocol Entity –	Entity that follows a set of rules and formats (semantic and syntactic) that determines the communication behavior of other entities. SOURCE: FIPS 188
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. SOURCE: SP 800-63

Proxy –	A proxy is an application that "breaks" the connection between client and server. The proxy accepts certain types of traffic entering or leaving a network and processes it and forwards it. This effectively closes the straight path between the internal and external networks. Making it more difficult for an attacker to obtain internal addresses and other details of the organization's internal network. Proxy servers are available for common Internet services; for example, an Hyper Text Transfer Protocol (HTTP) proxy used for Web access, and an Simple Mail Transfer Protocol (SMTP) proxy used for e-mail. SOURCE: SP 800-44
Proxy Agent –	A proxy agent is a software application running on a firewall or on a dedicated proxy server that is capable of filtering a protocol and routing it to between the interfaces of the device. SOURCE: SP 800-41
Proxy Server –	A server that sits between a client application, such as a web browser, and a real server. It intercepts all requests to the real server to see if it can fulfill the requests itself. If not, it forwards the request to the real server. SOURCE: SP 800-46
Pseudorandom number generator – (PRNG)	An algorithm that produces a sequence of bits that are uniquely determined from an initial value called a seed. The output of the PRNG "appears" to be random, i.e., the output is statistically indistinguishable from random values. A cryptographic PRNG has the additional property that the output is unpredictable, given that the seed is not known. SOURCE: SP 800-57
Pseudonym –	A subscriber name that has been chosen by the subscriber that is not verified as meaningful by identity proofing. SOURCE: SP 800-63
Public Key –	The public part of an asymmetric key pair that is typically used to verify signatures or encrypt data. SOURCE: SP 800-63

A cryptographic key that is used with a public key cryptographic algorithm. The public key is uniquely associated with an entity and may be made public. In an asymmetric (public) cryptosystem, the public key is associated with a private key. The public key may be known by anyone and, depending on the algorithm, may be used to—

1) Verify a digital signature that is signed by the corresponding private key,
2) Encrypt data that can be decrypted by the corresponding private key, or
3) Compute a piece of shared data.

SOURCE: SP 800-57

A cryptographic key used with a public key cryptographic algorithm, uniquely associated with an entity, and which may be made public; it is used to verify a digital signature; this key is mathematically linked with a corresponding private key.

SOURCE: FIPS 196

A cryptographic key used with a public key cryptographic algorithm that is uniquely associated with an entity and that may be made public.

SOURCE: FIPS 140-2

Public Key Certificate –

A digital document issued and digitally signed by the private key of a Certification Authority that binds the name of a subscriber to a public key. The certificate indicates that the subscriber identified in the certificate has sole control and access to the private key.

SOURCE: SP 800-63

A set of data that unambiguously identifies an entity, contains the entity's public key, and is digitally signed by a trusted third party (certification authority).

SOURCE: FIPS 196

A set of data that uniquely identifies an entity, contains the entity's public key, and is digitally signed by a trusted party, thereby binding the public key to the entity.

SOURCE: FIPS 140-2

Public Key (Asymmetric) Cryptographic Algorithm –

A cryptographic algorithm that uses two related keys, a public key and a private key. The two keys have the property that deriving the private key from the public key is computationally infeasible.

SOURCE: FIPS 140-2

Public key cryptography uses "key pairs," a public key and a mathematically related private key. Given the public key, it is infeasible to find the private key. The private key is kept secret while the public key may be shared with others. A message encrypted with the public key can only be decrypted with the private key. A message can be digitally signed with the private key, and anyone can verify the signature with the public key.

SOURCE: SP 800-46

Public Key Infrastructure – (PKI)

A set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.

SOURCE: SP 800-32

An architecture which is used to bind public keys to entities, enable other entities to verify public key bindings, revoke such bindings, and provide other services critical to managing public keys.

SOURCE: FIPS 196

Public Seed –

A starting value for a pseudorandom number generator. The value produced by the random number generator may be made public. The public seed is often called a "salt".

SOURCE: SP 800-56

Purge –

Rendering sanitized data unrecoverable by laboratory attack methods.

SOURCE: SP 800-88

Random Number Generator – (RNG)

A process used to generate an unpredictable series of numbers. Each individual value is called random if each of the values in the total population of values has an equal probability of being selected.

SOURCE: SP 800-57

Random Number Generators (RNGs) used for cryptographic applications typically produce a sequence of zero and one bits that may be combined into sub-sequences or blocks of random numbers. There are two basic classes: deterministic and nondeterministic. A deterministic RNG consists of an algorithm that produces a sequence of bits from an initial value called a seed. A nondeterministic RNG produces output that is dependent on some unpredictable physical source that is outside human control.

SOURCE: FIPS 140-2

Recipient Usage Period – The period of time during the cryptoperiod of a symmetric key when protected information is processed. The recipient usage period of the key is usually identical to the cryptoperiod of that key.

SOURCE: SP 800-57

Records – The recordings of evidence of activities performed or results achieved (e.g., forms, reports, test results) which serve as the basis for verifying that the organization and the information system are performing as intended. Also used to refer to units of related data fields (i.e., groups of data fields that can be accessed by a program and that contain the complete set of information on particular items).

SOURCE: SP 800-53; FIPS 200

Reference Monitor – The security engineering term for IT functionality that—
1) controls all access,
2) cannot be by-passed,
3) is tamper-resistant, and
4) provides confidence that the other three items are true.

SOURCE: SP 800-33

Registration – The process through which a party applies to become a subscriber of a Credentials Service Provider (CSP) and a Registration Authority validates the identity of that party on behalf of the CSP.

SOURCE: SP 800-63

Registration Authority – (RA) A trusted entity that establishes and vouches for the identity of a subscriber to a CSP. The RA 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).

SOURCE: SP 800-63

Organization responsible for assignment of unique identifiers to registered objects.

SOURCE: FIPS 188

Re-key (a certificate) – To change the value of a cryptographic key that is being used in a cryptographic system application; this normally entails issuing a new certificate on the new public key.

SOURCE: SP 800-32

Relying Party – An entity that relies upon the subscriber's credentials, typically to process a transaction or grant access to information or a system.

SOURCE: SP 800-63

Remediation – The act of correcting a vulnerability or eliminating a threat. Three possible types of remediation are installing a patch, adjusting configuration settings, or uninstalling a software application.

SOURCE: SP 800-40 Ver 2

Remediation Plan – A plan to perform the remediation of one or more threats or vulnerabilities facing an organization's systems. The plan typically includes options to remove threats and vulnerabilities and priorities for performing the remediation.

SOURCE: SP 800-40 Ver 2

Remote Access – Access by users (or information systems) communicating external to an information system security perimeter.

SOURCE: SP 800-18 Rev 1

Remote Maintenance – Maintenance activities conducted by individuals communicating external to an information system security perimeter.

SOURCE: SP 800-18 Rev 1

Renew (a certificate) – The act or process of extending the validity of the data binding asserted by a public key certificate by issuing a new certificate.

SOURCE: SP 800-32

Repository – A database containing information and data relating to certificates as specified in a CP; may also be referred to as a directory.

SOURCE: SP 800-32

Residual Risk – The remaining, potential risk after all IT security measures are applied. There is a residual risk associated with each threat.

SOURCE: SP 800-33

Responder – The entity that responds to the initiator of the authentication exchange.

SOURCE: FIPS 196

Responsible Individual – A trustworthy person designated by a sponsoring organization to authenticate individual applicants seeking certificates on the basis of their affiliation with the sponsor.

SOURCE: SP 800-32

Revoke a Certificate – To prematurely end the operational period of a certificate effective at a specific date and time.

SOURCE: SP 800-32

Rijndael – Cryptographic algorithm specified in the Advanced Encryption Standard (AES).

SOURCE: FIPS 197

Risk – The level of impact on agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.

SOURCE: SP 800-53; FIPS 200

Risk Analysis – The process of identifying the risks to system security and determining the likelihood of occurrence, the resulting impact, and the additional safeguards that mitigate this impact. Part of risk management and synonymous with risk assessment.

SOURCE: SP 800-27A

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

SOURCE: SP 800-53

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

SOURCE: SP 800-53

The process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system, and includes:

1) the conduct of a risk assessment;
2) the implementation of a risk mitigation strategy; and
3) employment of techniques and procedures for the continuous monitoring of the security state of the information system.

SOURCE: FIPS 200

The process of—
1) estimating potential losses due to the use of or dependence upon automated information system technology,
2) analyzing potential threats and system vulnerabilities that contribute to loss estimates, and
3) selecting cost effective safeguards that reduce risk to an acceptable level.

SOURCE: FIPS 191

Risk Mitigation – Risk mitigation involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls recommended from the risk assessment process.

SOURCE: SP 800-30

Risk Tolerance – The level of risk an entity is willing to assume in order to achieve a potential desired result.

SOURCE: SP 800-32

Root Certification Authority – In a hierarchical Public Key Infrastructure, the Certification Authority whose public key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain.

SOURCE: SP 800-32

Rootkit – A set of tools used by an attacker after gaining root-level access to a host to conceal the attacker's activities on the host and permit the attacker to maintain root-level access to the host through covert means.

SOURCE: SP 800-61

Round Key – Round keys are values derived from the Cipher Key using the Key Expansion routine; they are applied to the State in the Cipher and Inverse Cipher.

SOURCE: FIPS 197

Rule-Based Security Policy – A security policy based on global rules imposed for all subjects. These rules usually rely on a comparison of the sensitivity of the objects being accessed and the possession of corresponding attributes by the subjects requesting access.

SOURCE: SP 800-33

S-box – Non-linear substitution table used in several byte substitution transformations and in the Key Expansion routine to perform a one for one substitution of a byte value.

SOURCE: FIPS 197

S/MIME –

A set of specifications for securing electronic mail. Secure/ Multipurpose Internet Mail Extensions (S/MIME) is based upon the widely used MIME standard and describes a protocol for adding cryptographic security services through MIME encapsulation of digitally signed and encrypted objects. The basic security services offered by S/MIME are authentication, non-repudiation of origin, message integrity, and message privacy. Optional security services include signed receipts, security labels, secure mailing lists, and an extended method of identifying the signer's certificate(s).

SOURCE: SP 800-49

Safeguards –

Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Synonymous with security controls and countermeasures.

SOURCE: SP 800-53; CNSSI-4009 Adapted

Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices.

SOURCE: FIPS 200; CNSSI-4009 Adapted

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.

SOURCE: SP 800-63

Sandboxing –

A method of isolating application modules into distinct fault domains enforced by software. The technique allows untrusted programs written in an unsafe language, such as C, to be executed safely within the single virtual address space of an application. Untrusted machine interpretable code modules are transformed so that all memory accesses are confined to code and data segments within their fault domain. Access to system resources can also be controlled through a unique identifier associated with each domain.

SOURCE: SP 800-19

Sanitization –

Process to remove information from media such that information recovery is not possible. It includes removing all labels, markings, and activity logs.

SOURCE: SP 800-53; FIPS 200; CNSSI-4009 Adapted

Scanning –

Sending packets or requests to another system to gain information to be used in a subsequent attack.

SOURCE: SP 800-61

Scoping Guidance –

Provides organizations with specific technology-related, infrastructure-related, public access-related, scalability-related, common security control-related, and risk-related considerations on the applicability and implementation of individual security controls in the control baseline.

SOURCE: SP 800-53

Specific factors related to technology, infrastructure, public access, scalability, common security controls, and risk that can be considered by organizations in the applicability and implementation of individual security controls in the security control baseline.

SOURCE: FIPS 200

Secret Key –

A cryptographic key that is used with a secret key (symmetric) cryptographic algorithm, that is uniquely associated with one or more entities and is not be made public. The use of the term "secret" in this context does not imply a classification level, but rather implies the need to protect the key from disclosure.

SOURCE: SP 800-57

A cryptographic key that must be protected from unauthorized disclosure to protect data encrypted with the key.

SOURCE: FIPS 201

A cryptographic key that is uniquely associated with one or more entities. The use of the term "secret" in this context does not imply a classification level, but rather implies the need to protect the key from disclosure.

SOURCE: FIPS 198

A cryptographic key, used with a secret key cryptographic algorithm, that is uniquely associated with one or more entities and should not be made public.

SOURCE: FIPS 140-2

Secret Key (symmetric) Cryptographic Algorithm –

A cryptographic algorithm that uses a single secret key for both encryption and decryption.

SOURCE: FIPS 140-2

	This is the traditional method used for encryption. The same key is used for both encryption and decryption. Only the party or parties that exchange secret messages know the secret key. The biggest problem with symmetric key encryption is securely distributing the keys. Public key techniques are now often used to distribute the symmetric keys. SOURCE: SP 800-46
Secret Seed –	A secret value that used to initialize a pseudorandom number generator. The resulting value from the random number generator remains secret or private. SOURCE: SP 800-57
Secure/Multipurpose Internet Mail Extensions – (S/MIME)	A set of specifications for securing electronic mail. S/MIME is based upon the widely used MIME standard [MIME] and describes a protocol for adding cryptographic security services through MIME encapsulation of digitally signed and encrypted objects. The basic security services offered by S/MIME are authentication, non-repudiation of origin, message integrity, and message privacy. Optional security services include signed receipts, security labels, secure mailing lists, and an extended method of identifying the signer's certificate(s). SOURCE: SP 800-49
Secure Communication Protocol –	A communication protocol that provides the appropriate confidentiality, authentication and content integrity protection. SOURCE: SP 800-57
Secure Hash Algorithm – (SHA-1)	The Secure Hash Algorithm defined in Federal Information Processing Standard 180-1. SOURCE: SP 800-22
Secure Socket Layer and Transport Layer Security – (SSL and TSL)	Secure Sockets Layer is a protocol developed by Netscape for transmitting private documents via the Internet. SSL works by using a public key to encrypt data that's transferred over the SSL connection. Most web browsers support SSL, and many web sites use the protocol to obtain confidential user information, such as credit card numbers. By convention, URLs that require an SSL connection start with "https:" instead of "http:." TLS is an Internet standard based on SSL version 3.0. There are only very minor differences between SSL and TLS. SOURCE: SP 800-46

Security Accreditation –	The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls. SOURCE: SP 800-37
Security Assertion Markup Language – (SAML)	A specification for encoding security assertions in the Extensible Markup Language (XML). SOURCE: SP 800-63
Security Attribute –	A security-related quality of an object. Security attributes may be represented as hierarchical levels, bits in a bit map, or numbers. Compartments, caveats, and release markings are examples of security attributes. SOURCE: FIPS 188
Security Authorization –	The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls. SOURCE: SP 800-37
Security Category –	The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, or individuals. SOURCE: SP 800-53; FIPS 200; FIPS 199
Security Control Baseline –	The set of minimum security controls defined for a low-impact, moderate-impact, or high-impact information system. SOURCE: SP 800-53; FIPS 200
Security Control Enhancements –	Statements of security capability to: 1) build in additional, but related, functionality to a basic control; and/or 2) increase the strength of a basic control. SOURCE: SP 800-53
Security Controls –	The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. SOURCE: SP 800-53; FIPS 200; FIPS 199

Security Domain – A set of subjects, their information objects, and a common security policy.

SOURCE: SP 800-27A

A collection of entities to which applies a single security policy executed by a single authority.

SOURCE: FIPS 188

Security Goals – The five security goals are confidentiality, availability, integrity, accountability, and assurance.

SOURCE: SP 800-27A

Security Impact Analysis – The analysis conducted by an agency official, often during the continuous monitoring phase of the security certification and accreditation process, to determine the extent to which changes to the information system have affected the security posture of the system.

SOURCE: SP 800-53

Security Label – Explicit or implicit marking of a data structure or output media associated with an information system representing the FIPS 199 security category, or distribution limitations or handling caveats of the information contained therein.

SOURCE: SP 800-53

A marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource.

SOURCE: FIPS 188

Security Level – A hierarchical indicator of the degree of sensitivity to a certain threat. It implies, according to the security policy being enforced, a specific level of protection.

SOURCE: FIPS 188

Security Objective – Confidentiality, integrity, or availability.

SOURCE: SP 800-53; FIPS 200; FIPS 199

Security Perimeter – SEE Accreditation Boundary.

Security Plan – SEE System Security Plan.

Security Policy – The statement of required protection of the information objects.

SOURCE: SP 800-27A

	Security Policy is senior management's directives to create a computer security program, establish its goals, and assign responsibilities. SOURCE: SP 800-12
	A set of criteria for the provision of security services. It defines and constrains the activities of a data processing facility in order to maintain a condition of security for systems and data. SOURCE: FIPS 188
Security Requirements –	Requirements levied on an information system that are derived from laws, executive orders, directives, policies, instructions, regulations, or organizational (mission) needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted. SOURCE: SP 800-53
	Requirements levied on an information system that are derived from applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures, or organizational mission/business case needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted. SOURCE: FIPS 200
Security Service –	A capability that supports one, or many, of the security goals. Examples of security services are key management, access control, and authentication. SOURCE: SP 800-27A
Security Tag –	Information unit containing a representation of certain security-related information (e.g., a restrictive attribute bit map). SOURCE: FIPS 188
Senior Agency Information Security Officer –	Official responsible for carrying out the Chief Information Officer responsibilities under the Federal Information Security Management Act (FISMA) and serving as the Chief Information Officer's primary liaison to the agency's authorizing officials, information system owners, and information system security officers. SOURCE: SP 800-53; FIPS 200; 44 U.S.C., Sec. 3544
Sensitivity –	Used in this guideline to mean a measure of the importance assigned to information by its owner, for the purpose of denoting its need for protection. SOURCE: SP 800-60

Sensitivity Levels – A graduated system of marking (e.g., low, moderate, high) information and information processing systems based on threats and risks that result if a threat is successfully conducted.

SOURCE: FIPS 201

SHA-1 – SEE Secure Hash Algorithm.

Shared Secret – A secret used in authentication that is known to the claimant and the verifier.

SOURCE: SP 800-63

Signature – A recognizable, distinguishing pattern associated with an attack, such as a binary string in a virus or a particular set of keystrokes used to gain unauthorized access to a system.

SOURCE: SP 800-61

Signature Certificate – A public key certificate that contains a public key intended for verifying digital signatures rather than encrypting data or performing any other cryptographic functions.

SOURCE: SP 800-32

Signature Generation – Uses a digital signature algorithm and a private key to generate a digital signature on data.

SOURCE: SP 800-57

Signature Verification – Uses a digital signature algorithm and a public key to verify a digital signature.

SOURCE: SP 800-57

Signed Data – Data on which a digital signature is generated.

SOURCE: FIPS 196

Single-Hop Problem – The security risks resulting from an mobile software agent moving from its home platform to another platform.

SOURCE: SP 800-19

Smart Card – A credit card with a built-in microprocessor and memory that is used for identification or financial transactions. When inserted into a reader, the card transfers data to and from a central computer. A smart card is more secure than a magnetic stripe card and can be programmed to self-destruct if the wrong password is entered too many times.

SOURCE: SP 800-48

Sniffer – Software that observes and records network traffic.

SOURCE: SP 800-61

Social Engineering – An attempt to trick someone into revealing information (e.g., a password) that can be used to attack systems or networks.

SOURCE: SP 800-61

Software-Based Fault Isolation – A method of isolating application modules into distinct fault domains enforced by software. The technique allows untrusted programs written in an unsafe language, such as C, to be executed safely within the single virtual address space of an application. Untrusted machine interpretable code modules are transformed so that all memory accesses are confined to code and data segments within their fault domain. Access to system resources can also be controlled through a unique identifier associated with each domain.

SOURCE: SP 800-19

Split Knowledge – A procedure whereby a cryptographic key is handled as multiple key components from the time that the key or the separate key components are generated until the key components are combined for use. Each key component provides no knowledge of the ultimate key. The key may be created and then split into the key components, or may be created as separate key components. The key components are output from the generating cryptographic module(s) to separate entities for individual handling, and subsequently input separately into the intended cryptographic module and combined to form the ultimate key. Note: A suitable combination function is not provided by simple concatenation; e.g., it is not acceptable to form an 80-bit key by concatenating two 40-bit key components.

SOURCE: SP 800-57

A process by which a cryptographic key is split into multiple key components, individually sharing no knowledge of the original key, that can be subsequently input into, or output from, a cryptographic module by separate entities and combined to recreate the original cryptographic key.

SOURCE: FIPS 140-2

Spoofing – "IP spoofing" refers to sending a network packet that appears to come from a source other than its actual source.

SOURCE: SP 800-48

Involves—
1) the ability to receive a message by masquerading as the legitimate receiving destination, or
2) masquerading as the sending machine and sending a message to a destination.

SOURCE: FIPS 191

Spyware – Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge; a type of malicious code.

SOURCE: SP 800-53 Rev 1

SSL – SEE Secure Sockets Layer.

Standard – A published statement on a topic specifying characteristics, usually measurable, that must be satisfied or achieved in order to comply with the standard.

SOURCE: FIPS 201

Standard Topography – The format and information required to be displayed on a PIV card. Also known as the Mandatory Topography.

SOURCE: FIPS 201

State – Intermediate Cipher result that can be pictured as a rectangular array of bytes.

SOURCE: FIPS 197

Static Keys – Static keys are relatively long-lived and are common to a number of executions of a given algorithm.

SOURCE: SP 800-57

Steganography – The art and science of communicating in a way that hides the existence of the communication. For example, a child pornography image can be hidden inside another graphic image file, audio file, or other file format.

SOURCE: SP 800-72

Subject – The person whose identity is bound to a particular credential.

SOURCE: SP 800-63

Subordinate Certification Authority (CA) – In a hierarchical PKI, a Certification Authority whose certificate signature key is certified by another CA, and whose activities are constrained by that other CA.

SOURCE: SP 800-32

Subscriber –	A party who receives a credential or token from a CSP and becomes a claimant in an authentication protocol. SOURCE: SP 800-63
Subsystem –	A major subdivision or component of an information system consisting of information, information technology, and personnel that perform one or more specific functions. SOURCE: SP 800-18 Rev 1
Superior Certification Authority (CA) –	In a hierarchical PKI, a Certification Authority who has certified the certificate signature key of another CA, and who constrains the activities of that CA. SOURCE: SP 800-32
Symmetric Encryption Algorithm –	Encryption algorithms using the same secret key for encryption and decryption. SOURCE: SP 800-49
Symmetric Key –	A cryptographic key that is used to perform both the cryptographic operation and its inverse, for example to encrypt and decrypt, or create a message authentication code and to verify the code. SOURCE: SP 800-63 A single cryptographic key that is used with a secret (symmetric) key algorithm. SOURCE: SP 800-21 [2nd Ed]
System –	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. ALSO SEE Information System. SOURCE: SP 800-53
System Administrator –	A person who manages the technical aspects of a system. SOURCE: SP 800-40 Ver 2
System Development Life Cycle – (SDLC)	The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal that instigates another system initiation. SOURCE: SP 800-34

System Integrity – The quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation of the system, whether intentional or accidental.

SOURCE: SP 800-27A; CNSSI-4009 Adapted

System Interconnection – The direct connection of two or more IT systems for the purpose of sharing data and other information resources.

SOURCE: SP 800-47

System-specific Security Control – A security control for an information system that has not been designated as a common security control.

SOURCE: SP 800-53

System Security Plan – Formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements.

SOURCE: SP 800-53; FIPS 200

System Software – The special software within the cryptographic boundary (e.g., operating system, compilers or utility programs) designed for a specific computer system or family of computer systems to facilitate the operation and maintenance of the computer system, and associated programs, and data.

SOURCE: FIPS 140-2

Technical Controls – The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.

SOURCE: SP 800-53; FIPS 200

Technical non-repudiation – The contribution of public key mechanisms to the provision of technical evidence supporting a non-repudiation security service.

SOURCE: SP 800-32

Tempest – A name referring to the investigation, study, and control of unintentional compromising emanations from telecommunications and automated information systems equipment.

SOURCE: FIPS 140-2

Template – A biometric image data record.

SOURCE: FIPS 201

Threat –

Any circumstance or event with the potential to adversely impact agency operations (including mission, functions, image, or reputation), agency assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

SOURCE: SP 800-53; CNSSI-4009 Adapted

Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability.

SOURCE: FIPS 200; CNSSI-4009 Adapted

Threat Agent/Source –

Either:
1) intent and method targeted at the intentional exploitation of a vulnerability; or
2) a situation and method that may accidentally trigger a vulnerability.

SOURCE: SP 800-53

Threat Analysis –

The examination of threat sources against system vulnerabilities to determine the threats for a particular system in a particular operational environment.

SOURCE: SP 800-27A

Threat Assessment –

Formal description and evaluation of threat to an information system.

SOURCE: SP 800-53; CNSSI-4009

Threat Source –

The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability.

SOURCE: FIPS 200

Either:
1) intent and method targeted at the intentional exploitation of a vulnerability; or
2) a situation and method that may accidentally trigger a vulnerability. Synonymous with threat agent.

SOURCE: SP 800-37

Token –

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

SOURCE: SP 800-63

Topology –	The physical, non-logical features of a card. A card may have either standard or enhanced topography. SOURCE: FIPS 201
Total Risk –	The potential for the occurrence of an adverse event if no mitigating action is taken (i.e., the potential for any applicable threat to exploit a system vulnerability). SOURCE: SP 800-16
Tracking Cookie –	A cookie placed on a user's computer to track the user's activity on different Web sites, creating a detailed profile of the user's behavior. SOURCE: SP 800-83
Traffic Analysis –	A form of passive attack in which an intruder observes information about calls (although not necessarily the contents of the messages) and makes inferences, e.g. from the source and destination numbers, or frequency and length of the messages. SOURCE: SP 800-24
Training (Information Security) –	Training strives to produce relevant and needed (information) security skills and competencies. SOURCE: SP 800-50
Training Assessment –	An evaluation of the training efforts. SOURCE: SP 800-16
Training Effectiveness –	A measurement of what a given student has learned from a specific course or training event. SOURCE: SP 800-16
Training Effectiveness Evaluation –	Information collected to assist employees and their supervisors in assessing individual students' subsequent on-the-job performance, to provide trend data to assist trainers in improving both learning and teaching, and to be used in return-on-investment statistics to enable responsible officials to allocate limited resources in a thoughtful, strategic manner among the spectrum of IT security awareness, security literacy, training, and education options for optimal results among the workforce as a whole. SOURCE: SP 800-16
Transport Layer Security – (TLS)	An authentication and security protocol widely implemented in browsers and web servers. SOURCE: SP 800-63

Triple DES – An implementation of the Data Encryption Standard (DES) algorithm that uses three passes of the DES algorithm instead of one as used in ordinary DES applications. Triple DES provides much stronger encryption than ordinary DES but it is less secure than AES.

SOURCE: SP 800-46

Trojan Horse – A non-self-replicating program that seems to have a useful purpose, but in reality has a different, malicious purpose.

SOURCE: SP 800-61

Trust Anchor – A public key and the name of a certification authority that is used to validate the first certificate in a sequence of certificates. The trust anchor public key is used to verify the signature on a certificate issued by a trust anchor certification authority. The security of the validation process depends upon the authenticity and integrity of the trust anchor. Trust anchors are often distributed as self-signed certificates.

SOURCE: SP 800-57

Trust List – The collection of trusted certificates used by Relying Parties to authenticate other certificates.

SOURCE: SP 800-32

Trusted Agent – Entity authorized to act as a representative of an Agency in confirming Subscriber identification during the registration process. Trusted Agents do not have automated interfaces with Certification Authorities.

SOURCE: SP 800-32

Trusted Certificate – A certificate that is trusted by the Relying Party on the basis of secure and authenticated delivery. The public keys included in trusted certificates are used to start certification paths. Also known as a "trust anchor".

SOURCE: SP 800-32

Trusted Path – A mechanism by which a user (through an input device) can communicate directly with the security functions of the information system with the necessary confidence to support the system security policy. This mechanism can only be activated by the user or the security functions of the information system and cannot be imitated by untrusted software.

SOURCE: SP 800-53

A means by which an operator and a target of evaluation security function can communicate with the necessary confidence to support the target of evaluation security policy.

SOURCE: FIPS 140-2; CNSSI-4009 Adapted

Trusted Timestamp – A digitally signed assertion by a trusted authority that a specific digital object existed at a particular time.

SOURCE: SP 800-32

Trustworthiness – The attribute of a person or organization that provides confidence to others of the qualifications, capabilities, and reliability of that entity to perform specific tasks and fulfill assigned responsibilities.

SOURCE: SP 800-79

Trustworthy System – Computer hardware, software and procedures that—
1) are reasonably secure from intrusion and misuse;
2) provide a reasonable level of availability, reliability, and correct operation;
3) are reasonably suited to performing their intended functions; and
4) adhere to generally accepted security procedures.

SOURCE: SP 800-32

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.

SOURCE: SP 800-63

Unauthorized Access – A person gains logical or physical access without permission to a network, system, application, data, or other resource.

SOURCE: SP 800-61

Occurs when a user, legitimate or unauthorized, accesses a resource that the user is not permitted to use.

SOURCE: FIPS 191

Unauthorized Disclosure – An event involving the exposure of information to entities not authorized access to the information.

SOURCE: SP 800-57; CNSSI-4009 Adapted

Unsigned data – Data included in an authentication token, in addition to a digital signature.

SOURCE: FIPS 196

Update (a Certificate) – The act or process by which data items bound in an existing public key certificate, especially authorizations granted to the subject, are changed by issuing a new certificate.

SOURCE: SP 800-32

User – Individual or (system) process authorized to access an information system.

SOURCE: SP 800-53; FIPS 200; CNSSI-4009

An individual or a process (subject) acting on behalf of the individual that accesses a cryptographic module in order to obtain cryptographic services.

SOURCE: FIPS 140-2

User Initialization – A stage in the lifecycle of keying material; the process whereby a user initializes its cryptographic application (e.g., installing and initializing software and hardware).

SOURCE: SP 800-57

User Registration – A stage in the lifecycle of keying material; a process whereby an entity becomes a member of a security domain.

SOURCE: SP 800-57

Valid Data Element – A payload, an associated data string, or a nonce that satisfies the restrictions of the formatting function.

SOURCE: SP 800-38C

Validation – The process of demonstrating that the system under consideration meets in all respects the specification of that system.

SOURCE: FIPS 201; INCITS/M1-040211

Verification – The process of affirming that a claimed identity is correct by comparing the offered claims of identity with previously proven information stored in the identity card or PIV system. See Identity Verification.

SOURCE: FIPS 201

Verified Name – A subscriber name that has been verified by identity proofing.

SOURCE: SP 800-63

Verifier – An entity that verifies the claimant's identity by verifying the claimant's possession of a token using an authentication protocol. To do this, the verifier may also need to validate credentials that link the token and identity and check their status.

SOURCE: SP 800-63

	An entity which is or represents the entity requiring an authenticated identity. A verifier includes the functions necessary for engaging in authentication exchanges. SOURCE: FIPS 196
Verifier Impersonation Attack –	An attack where the attacker impersonates the verifier in an authentication protocol, usually to learn a password. SOURCE: SP 800-63
Victim –	A machine that is attacked. SOURCE: SP 800-61
Virtual Private Network – (VPN)	A virtual private network is a logical network that is established, at the application layer of the Open Systems Interconnection (OSI) model, over an existing physical network and typically does not include every node present on the physical network. SOURCE: SP 800-46
Virus –	A self-replicating program that runs and spreads by modifying other programs or files SOURCE: SP 800-61
Virus Hoax –	An urgent warning message about a nonexistent virus. SOURCE: SP 800-61
Vulnerability –	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. SOURCE: SP 800-53; FIPS 200; CNSSI-4009 Adapted
Vulnerability Assessment –	Formal description and evaluation of the vulnerabilities in an information system. SOURCE: SP 800-53; CNSSI-4009
Warez –	A term widely used by hackers to denote illegally copied and distributed commercial software from which all copy protection has been removed. Warez often contains viruses, Trojans and other malicious code and thus is very risky to download and use (legal issues notwithstanding). SOURCE: SP 800-46
Warm Site –	An environmentally conditioned workspace that is partially equipped with IT and telecommunications equipment to support relocated IT operations in the event of a significant disruption. SOURCE: SP 800-34

Web Bug –	Tiny images, invisible to a user, placed on web sites in such a way that they allow third parties to track use of web servers and collect information about the user, including IP address, Host name, browser type and version, operating system name and version, and web browser cookie. SOURCE: SP 800-46
Wired Equivalent Privacy – (WEP)	Wired Equivalent Privacy, a security protocol for wireless local area networks (WLANs) defined in the 802.11b standard. WEP was intended to provide the same level of security as that of a wired LAN. SOURCE: SP 800-46
Wireless Application Protocol – (WAP)	A standard for providing cellular telephones, pagers, and other handheld devices with secure access to e-mail and text-based Web pages SOURCE: SP 800-48
Worm –	A self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself. SOURCE: SP 800-61
Write-Blocker –	A device that allows investigators to examine media while preventing data writes from occurring on the subject media. SOURCE: SP 800-72
X.509 Certificate –	The International Organization for Standardization/International Telecommunication Union – Standardization Department (ISO/ITU-T) X.509 standard defined two types of certificates – the X.509 public key certificate, and the X.509 attribute certificate. Most commonly (including this document), an X.509 certificate refers to the X.509 public key certificate. SOURCE: SP 800-57
X.509 Public Key Certificate –	The public key for a user (or device) and a name for the user (or device), together with some other information, rendered unforgeable by the digital signature of the certification authority that issued the certificate, encoded in the format defined in the ISO/ITU-T X.509 standard. SOURCE: SP 800-57
Zeroization –	A method of erasing electronically stored data, cryptographic keys, and CSPs by altering or deleting the contents of the data storage to prevent recovery of the data. SOURCE: FIPS 140-2

Zombie – A program that is installed on a system to cause it to attack other systems.

SOURCE: SP 800-83

NON-NIST REFERENCES

40 U.S.C., Sec. 11101	U.S. Code, Title 40 – Public Buildings, Property, and Works, Subtitle III – Information Technology Management, Chapter 111 – General, Section 11101. Definitions.
40 U.S.C., Sec. 11331	U.S. Code, Title 40 – Public Buildings, Property, and Works, Subtitle III – Information Technology Management, Chapter 113 – Responsibility for Acquisitions of Information Technology, Subchapter III – Other Responsibilities, Section 11331. Responsibilities for Federal information systems standards.
41 U.S.C., Sec. 403	Title 41 – Public Contracts, Chapter 7 – Office of Federal Procurement Policy, Section 403. Definitions.
44 U.S.C., Sec. 3502	U.S. Code, Title 44 – Public Printing and Documents, Chapter 35 – Coordination of Federal Information Policy, Subchapter I – Federal Information Policy, Section 3502. Definitions.
44 U.S.C., Sec. 3541	U.S. Code, Title 44 – Public Printing and Documents, Chapter 35 – Coordination of Federal Information Policy, Subchapter III – Information Security, Section 3541. Purposes.
44 U.S.C., Sec. 3542	U.S. Code, Title 44 – Public Printing and Documents, Chapter 35 – Coordination of Federal Information Policy, Subchapter III – Information Security, Section 3542. Definitions.
44 U.S.C., Sec. 3544	U.S. Code, Title 44 – Public Printing and Documents, Chapter 35 – Coordination of Federal Information Policy, Subchapter III – Information Security, Section 3544. Federal agency responsibilities.
47 C.F.R., Part 64, App A	Code of Federal Regulations, Title 47 – Telecommunication, Chapter I – Federal Communications Commission, Subchapter B – Common Carrier Services, Part 64 – Miscellaneous Rules Relating to Common Carriers, Appendix A to Part 64 – Telecommunications Service Priority (TSP) System for National Security Emergency Preparedness (NSEP)
ANSDIT	*American National Standard Dictionary for Information Technology (ANSDIT),* ANSI X3.197-1996, and the draft of the Millennial Edition of ANSDIT 2000.
CNSSI-4009	The Committee on National Security Systems Instruction No 4009*"National Information Assurance Glossary."*
E.O. 13292	Executive Office of the President, Executive Order 13292— Further Amendment to Executive Order 12958, as Amended, Classified National Security Information, March 25, 2003.

INCITS/M1-040211	InterNational Committee for Information Technology Standards (INCITS) Technical Committee M1, Biometrics, *Biometric Profile - Interoperability and Data Interchange - Biometrics-Based Verification and Identification of Transportation Workers*. April 23, 2004.
OMB Circular A-130, App. III	U.S. Office of Management and Budget, Circular No. A-130 Revised, (Transmittal Memorandum No. 4), Appendix III, Security of Federal Automated information Resources. November 28, 2000.
OMB Memorandum 02-01	U.S. Office of Management and Budget, Memorandum 02-01, Guidance for Preparing and Submitting Security Plans of Action and Milestones. October 17, 2001.
OMB Memorandum 03-22	U.S. Office of Management and Budget, Memorandum 03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002. September 29, 2003.
Public Law 104-106 Sec. 5125(b)	S. 1124, Division E [Public Law 104-106], 104th U.S. Cong., Information Technology Management Reform Act, February 10, 1996. Section 5125(b).