GLOSSARY OF CYBER SECURITY TERMS
(v.4)

#- Ac

# #

1xRTT (Single Carrier (1x) Radio Transmission Technology) - A wireless communications protocol used for connections to *networks* by devices such as laptop computers. 1xRTT has the capability of providing data transfer speeds of up to 144 thousand *bps*.

403 Forbidden - The web server is replying with a 403 Forbidden response when it detects that someone is trying to access restricted pages on the web server.

A

Access - Ability and means to communicate or interact with a system; to use system resources to handle information; to gain knowledge of the information the system contains; or to control system components and functions.

Access authority - Entity responsible for monitoring and granting access privileges for other authorized entities.

Access control - The process of granting or denying specific requests:

- For obtaining and using information and related information processing services; and
- To enter specific physical facilities (e.g., Federal buildings, military establishments, and border crossing entrances).

Access Control List (ACL) - A mechanism that implements access control for a system resource by enumerating the system entities that are permitted to access the resource and stating, either implicitly or explicitly, the access modes granted to each entity.

Access control mechanism - Security safeguards (i.e., *hardware and software features, physical controls, operating procedures, management procedures, and various combinations of these*) designed to detect and deny unauthorized access and permit authorized access to an information system.

Access level – is a category within a given security classification, limiting entry or system connectivity to only authorized persons.

Access list - Roster of individuals with authorized admittance to a controlled area.

Access profile - Association of a user with a list of protected objects the user may access.

Access type- The privilege to perform action on an object; Read, write, execute, append, modify, delete, and create are examples of access types.

Account harvesting - Is the process of collecting all the legitimate account names on a system.

Accountability – Is the principle that an individual is entrusted to safeguard and control equipment, keying material, and information and is answerable to proper authority for the loss or misuse of that equipment or information.

Accounting Legend Code (ALC) - Numeric code used to indicate the minimum accounting controls required for items of accountable COMSEC material within the COMSEC Material Control System.

Accounting number - Number assigned to an item of COMSEC material to facilitate its control.

Accreditation - Formal declaration by a Designated Accrediting Authority (DAA) or Principal Accrediting Authority (PAA) that an information system is approved to operate at an acceptable level of risk, based on the implementation of an approved set of technical, managerial, and procedural safeguards.

Accreditation boundary - Identifies the information resources covered by an accreditation decision, as distinguished from separately accredited information resources that are interconnected or with which information is exchanged via messaging.

Accreditation package - Product comprised of a System Security Plan (SSP) and a report documenting the basis for the accreditation decision.

Accrediting Authority – This is synonymous with Designated Accrediting Authority (DAA). See also Authorizing Official.

Active attack – Is an attack that alters a system or data.

Active content - Is software in various forms that is able to automatically carry out or trigger actions on a computer platform without the intervention of a user.

Add-on security - Incorporation of new or additional hardware, software, or firmware safeguards in an operational information system.

Adequate security – is a security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.

Advanced Encryption Standard (AES) – is a U.S. Government-approved cryptographic algorithm that can be used to protect electronic data. This algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information.

Advanced Key Processor (AKP) - A cryptographic device that performs all cryptographic functions for a management client node and contains the interfaces to:

1. Exchange information with a client platform;
2. Interact with fill devices; and
3. Connect a client platform securely to the primary services node (PRSN).

Advanced Research Projects Agency Network (ARPANet) – The precursor to the *Internet*. This was developed in the late 60's and early 70's by the US Department of Defense as an experiment in wide-area-networking to connect together computers that were each running different system so that people at one location could use computing resources from another location.

Advisory - Notification of significant new trends or developments regarding the threat to the information systems of an organization. This notification may include analytical insights into trends, intentions, technologies, or tactics of an adversary targeting information systems.

Adware – A general term used for software that invades your computer in the form of persistent pop-ups. An adware is defined as *a form of spyware that enters your computer from an Internet download.*

Alert- Notification that a specific attack has been directed at an organization's information systems.

Alternate COMSEC custodian - Individual designated by proper authority to perform the duties of the COMSEC custodian during the temporary absence of the COMSEC custodian.

American Standard Code for Information Interchange (ASCII) - This is the defacto world-wide standard for the code numbers used by computers to represent all the upper and lower-case Latin letters, numbers, punctuation, etc. There are 128 standard ASCII codes each of which can be represented by a 7 digit binary number: 0000000 through 1111111.

Anonymous - A loosely affiliated collective of "hacktivists" who engage ideologically motivated cyber-attacks against corporate and governmental targets through web site disruptions and defacements, and the theft and release of sensitive documents and personal information. These attacks are often motivated by perceived violations of social, political or environmental norms.

Anti-jam - Countermeasures ensuring that transmitted information can be received despite deliberate jamming attempts.

Anti-spoof - Countermeasures taken to prevent the unauthorized use of legitimate Identification & Authentication (I&A) data, however it was obtained, to mimic a subject different from the attacker.

Ap-As

Apache - The most common web server (or *HTTP* server) software on the Internet. Designed as a set of modules, enabling administrators to choose which features they wish to use and making it easy to add features to meet specific needs including handling protocols other than the web-standard *HTTP*.

Applet - A small *Java* program that can be embedded in an *HTML* page. Applets differ from full-fledged Java applications in that they are not allowed to access certain resources on the local computer, such as files and serial devices (modems, printers, etc.), and are prohibited from communicating with most other computers across a network. The common rule is that an applet can only make an Internet connection to the computer from which the applet was sent.

Application - Software program that performs a specific function directly for a user and can be executed without access to system control, monitoring, or administrative privileges. It also performs automated functions for a user, such as word processing, spreadsheets, graphics, presentations and databases—as opposed to operating system (OS) software.

Approval to Operate (ATO) - The official management decision issued by a DAA or PAA to authorize operation of an information system and to explicitly accept the residual risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals.

Asset - A major application, general support system, high impact program, physical plant, mission critical system, personnel, equipment, or a logically related group of systems.

Assurance - Measure of confidence that the security features, practices, procedures, and architecture of an information system accurately mediates and enforces the security policy.

Assured information sharing - The ability to confidently share information with those who need it, when and where they need it, as determined by operational need and an acceptable level of security risk.

Assured software - Computer application that has been designed, developed, analyzed and tested using processes, tools, and techniques that establish a level of confidence in it.

Asymmetric Digital Subscriber Line (ADSL) - A *DSL* line where the upload speed is different from the download speed. Usually the download speed is much greater.

Asynchronous JavaScript and XML (AJAX) - A way of including content in a *web page* in which *JavaScript* code in the web page fetches some data from a server and displays it without re-fetching the entire surrounding page at the same time (hence the 'Asynchronous') . A simple example of Ajax would be a weather-forecast box in the middle of a web page. Ajax could be used to populate the box every 5 minutes without needing to refresh the surrounding page.

Attack - Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself.

Attack Sensing and Warning (AS&W) - Detection, correlation, identification, and characterization of intentional unauthorized activity with notification to decision makers so that an appropriate response can be developed.

Attack signature - A characteristic byte pattern used in malicious code or an indicator, or set of indicators that allows the identification of malicious network activities.

Attribute-based access control - Access control based on attributes associated with and about subjects, objects, targets, initiators, resources, or the environment. An access control rule set defines the combination of attributes under which an access may take place.

Attribute-based authorization - A structured process that determines when a user is authorized to access information, systems, or services based on attributes of the user and of the information, system, or service.

Audit - Independent review and examination of records and activities to assess the adequacy of system controls and ensure compliance with established policies and operational procedures.

Audit log – Is a chronological record of system activities; Includes records of system accesses and operations performed in a given period.

Audit reduction tools – Pre-processors 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.

Audit trail – Is a chronological record that reconstructs and examines the sequence of activities surrounding or leading to a specific operation, procedure, or event in a security relevant transaction from inception to final result.

Authenticate - To verify the identity of a user, user device, or other entity.

Authentication - The process of verifying the identity or other attributes claimed by or assumed of an entity (user, process, or device), or to verify the source and integrity of data; Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

Authentication mechanism – Is a hardware or software-based algorithm that forces users, devices, or processes to prove their identity before accessing data on an information system.

Au

Authentication period - The maximum acceptable period between any initial authentication process and subsequent re-authentication processes during a single terminal session or during the period data is being accessed.

Authentication protocol – Is a well specified message exchange process between a claimant and a verifier that enables the verifier to confirm the claimant's identity.

Authenticator - The means used to confirm the identity of a user, process, or device (e.g., user password or token).

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.

Authority - Person(s) or established bodies with rights and responsibilities to exert control in an administrative sphere.

Authorization - Access privileges granted to a user, program, or process or the act of granting those privileges.

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

Authorization boundary - All components of an information system to be authorized for operation by an authorizing official and excludes separately authorized systems, to which the information system is connected.

Authorized vendor - Manufacturer of information assurance equipment authorized to produce quantities in excess of contractual requirements for direct sale to eligible buyers.

Authorizing Official - Senior (federal) official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.

Authorizing Official Designated Representative - An organizational official acting on behalf of an authorizing official in carrying out and coordinating the required activities associated with security authorization.

Automated security monitoring - Use of automated procedures to ensure security controls are not circumvented or the use of these tools to track actions taken by subjects suspected of misusing the information system.

Automatic remote rekeying - Procedure to rekey distant cryptographic equipment electronically without specific actions by the receiving terminal operator. See manual remote rekeying.

Availability - The property of being accessible and useable upon demand by an authorized entity; ensuring timely and reliable access to and use of information.

B

Backbone - A primary transit network or series of networks, designed to carry data between different local area networks. A backbone generally has greater data carrying capacity, or "bandwidth", than the networks connected to it. The Internet Backbone is the interconnection of high-speed networks, primarily government, commercial telecommunications and academic networks that route data for public Internet users.

Back door - Typically unauthorized hidden software or hardware mechanism used to circumvent security controls; a method of regaining remote control of a victim's computer by reconfiguring installed legitimate software or the installation of a specialized program designed to allow access under attacker-defined conditions. Trojan horse programs and rootkits often contain backdoor components.

Backup - Copy of files and programs made to facilitate recovery, if necessary.

Bandwidth - How much stuff you can send through a connection; usually measured in bits-per-second (*bps*.) A full page of English text is about 16,000 bits. A fast modem can move about 57,000 bits in one second. Full-motion full-screen video would require roughly 10,000,000 bits-per-second, depending on compression.

Banner - Display on an information system that sets parameters for system or data use.

Baseline - Hardware, software, databases, and relevant documentation for an information system at a given point in time.

Bastion host - A special purpose computer on a network specifically designed and configured to withstand attacks.

Baud - In common usage the "baud" of a *modem* is how many *bits* it can send or receive per second. Technically, baud is the number of times per second that the carrier signal shifts value - for example a 1200 bit-per-second modem actually runs at 300 baud, but it moves 4 bits per baud (4 x 300= 1200 bits per second).

Be-Bi

Benign environment - A non-hostile location protected from external hostile elements by physical, personnel, and procedural security countermeasures.

Binary - Information consisting entirely of ones and zeroes; also, commonly used to refer to files that are not simply text files (e.g. images).

Binding - Process of associating two or more related elements of information.

Biometrics - Measurable physical characteristics or personal behavioral traits used to identify, or verify the claimed identity, of an individual. Facial images, fingerprints, and handwriting samples are all examples of biometrics.

Bit - A contraction of the term Binary Digit. This is the smallest unit of information in a binary system of notation; the smallest unit of information storage, a contraction of the term "binary digit."

- **Nibble**
  - A Nibble is 4 bits.
- **Byte**
  - A Byte is 8 bits.
- **Kilobyte (KB)**
  - A Kilobyte is 1,024 bytes.
- **Megabyte (MB)**
  - A Megabyte is 1,048,576 bytes or 1,024 Kilobytes
    - **873** pages of plaintext (1,200 characters)
    - **4** books (200 pages or 240,000 characters)
- **Gigabyte (GB)**
  - A Gigabyte is 1,073,741,824 (2^{30}) bytes. 1,024 Megabytes or 1,048,576 Kilobytes.
    - **894,784** pages of plaintext (1,200 characters)
    - **4,473** books (200 pages or 240,000 characters)
    - **341** digital pictures (with 3MB average file size)
    - **256** MP3 audio files (with 4MB average file size)
    - **1** 650MB CD
- **Terabyte (TB)**
  - A Terabyte is 1,099,511,627,776 (2^{40}) bytes, 1,024 Gigabytes, or 1,048,576 Megabytes.
    - **916,259,689** pages of plaintext (1,200 characters)
    - **4,581,298** books (200 pages or 240,000 characters)
    - **349,525** digital pictures (with 3MB average file size)
    - **262,144** MP3 audio files (with 4MB average file size)
    - **1,613** 650MB CD's
    - **233** 4.38GB DVD's
    - **40** 25GB Blu-ray discs
- **Petabyte (PB)**
  - A Petabyte is 1,125,899,906,842,624 (2^{50}) bytes, 1,024 Terabytes, or 1,048,576 Gigabytes.
    - **938,249,922,368** pages of plaintext (1,200 characters)
    - **4,691,249,611** books (200 pages or 240,000 characters)
    - **357,913,941** digital pictures (with 3MB average file size)
    - **268,435,456** MP3 audio files (with 4MB average file size)
    - **1,651,910** 650MB CD's
    - **239,400** 4.38GB DVD's
    - **41,943** 25GB Blu-ray discs
- **Exabyte (EB)**
  - A Exabyte is 1,152,921,504,606,846,976 (2^{60}) bytes, 1,024 Petabytes, or 1,048,576 Terabytes.
    - **960,767,920,505,705** pages of plaintext (1,200 characters)
    - **4,803,839,602,528** books (200 pages or 240,000 characters)
    - **366,503,875,925** digital pictures (with 3MB average file size)
    - **274,877,906,944** MP3 audio files (with 4MB average file size)
    - **1,691,556,350** 650MB CD's

    - **245,146,535** 4.38GB DVD's
    - **42,949,672** 25GB Blu-ray discs
- **Zettabyte (ZB)**
  - A Zettabyte is 1,180,591,620,717,411,303,424 (2^{70}) bytes, 1,024 Exabytes, or 1,048,576 Petabytes.
    - **983,826,350,597,842,752** pages of plaintext (1,200 characters)
    - **4,919,131,752,989,213** books (200 pages or 240,000 characters)
    - **375,299,968,947,541** digital pictures (with 3MB average file size)
    - **281,474,976,710,656** MP3 audio files (with 4MB average file size)
    - **1,732,153,702,834** 650MB CD's
    - **251,030,052,003** 4.38GB DVD's
    - **43,980,465,111** 25GB Blu-ray discs
- **Yottabyte (YB)**
  - A Yottabyte is 1,208,925,819,614,629,174,706,176 (2^{80}) bytes, 1,024 Zettabytes, or 1,048,576 Exabytes.
    - **1,007,438,183,012,190,978,921** pages of plaintext (1,200 characters)
    - **5,037,190,915,060,954,894** books (200 pages or 240,000 characters)
    - **384,307,168,202,282,325** digital pictures (with 3MB average file size)
    - **288,230,376,151,711,744** MP3 audio files (with 4MB average file size)
    - **1,773,725,391,702,841** 650MB CD's
    - **257,054,773,251,740** 4.38GB DVD's
    - **45,035,996,273,704** 25GB Blu-ray discs

Bit error rate - Ratio between the number of bits incorrectly received and the total number of bits transmitted in a telecommunications system.

Bits per second – This is a measurement of how fast data is moved from one place to another. A 56K *modem* can move about 57,000 bits per second.

Black - Designation applied to encrypted information and the information systems, the associated areas, circuits, components, and equipment processing that information.

Black core – This is a communication network architecture in which user data traversing a global IP network is end-to-end encrypted at the IP layer; also related to striped core.

Black hat – Is a computer hacker whose intent is to cause damage or to take other unauthorized or illegal actions against a victim.

Blacklisting - The process of the system invalidating a user ID based on the user's inappropriate actions. A blacklisted user ID cannot be used to log on to the system, even with the correct authenticator. Blacklisting and lifting of a blacklisting are both security-relevant events. Blacklisting also applies to blocks placed against IP addresses to prevent inappropriate or unauthorized use of internet resources.

Blended attack – This is a hostile action that spreads malicious code via multiple methods.

Bl-Br

Blog - Short for "Web log," a blog is usually defined as an online diary or journal. It is usually updated frequently and offered in a dated log format with the most recent entry at the top of the page. It often contains links to other websites along with commentary about those sites or specific subjects, such as politics, news, pop culture or computers.

Blue Team - The group responsible for defending an enterprise's use of information systems by maintaining its security posture against a group of mock attackers (i.e., the Red Team). Typically the Blue Team and its supporters must defend against real or simulated attacks:

1. over a significant period of time;
2. in a representative operational context (e.g., as part of an operational exercise), and
3. according to rules established and monitored with the help of a neutral group refereeing the simulation or exercise (i.e., the White Team);

Body of Evidence (BoE) - The set of data that documents the information system's adherence to the security controls applied. The BoE will include a Requirements Verification Traceability Matrix (RVTM) delineating where the selected security controls are met and evidence to that fact can be found. The BoE content required by an Authorizing Official will be adjusted according to the impact levels selected.

Botnet – This is a network consisting of thousands of machines that have been infected with Trojan horse viruses and are now controlled by criminals.

Bounce Back - Bounce-back refers to the return of an email message because of an error in its address or delivery.

Boundary protection - Monitoring and control of communications at the external boundary of an information system to prevent and detect malicious and other unauthorized communications, through the use of boundary protection devices (e.g., proxies, gateways, routers, firewalls, guards, encrypted tunnels).

Boundary protection device - A device with appropriate mechanisms that facilitates the adjudication of different security policies for interconnected systems; A device with appropriate mechanisms that: (i) facilitates the adjudication of different interconnected system security policies (e.g., controlling the flow of information into or out of an interconnected system); and/or (ii) provides information system boundary protection.

Broadband - Sometimes referred to as high-speed internet, broadband is an 'always on' fast connection to the internet. Today there are a wide variety of broadband technologies available in most areas of Australia. Broadband can be fire optic, ADSL, DSL or wireless.

Browser - A client software program that can retrieve and display information from servers on the World Wide Web.

Browsing - Act of searching through information system storage or active content to locate or acquire information, without necessarily knowing the existence or format of information being sought.

Brute Force Attack – Is an exhaustive password-cracking procedure that tries all possibilities, one by one.

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.

Bulk encryption – Is a simultaneous encryption of all channels of a multi-channel telecommunications link.

Bulletin board System (BBS) - A computerized meeting and announcement system that allows people to carry on discussions, upload and download files, and make announcements without the people being connected to the computer at the same time. In the early 1990's there were many thousands of BBS's around the world, most were very small, running on a single IBM clone PC with 1 or 2 phone lines. Some were very large and the line between a BBS and a system like AOL gets crossed at some point, but it is not clearly drawn.

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.

Business Impact Analysis (BIA) - An analysis of an enterprise's requirements, processes, and interdependencies used to characterize information system contingency requirements and priorities in the event of a significant disruption.

Byte - A fundamental unit of computer storage. Usually holds one character of information and usually means 8 bits.

C

C2 - Command and control. The term, in the context of computer network operations, often describes a communications method or a component thereof to maintain remote control of an operational asset, such as a compromised computer.

Cache - A place to store files locally for quicker access. Caches, which can be temporary or permanent, are used to speed up data transfer. Memory and disk caches are used in every computer to speed up instruction execution and data retrieval. Material in caches often remains even after it has been used or viewed.

Call back - Procedure for identifying and authenticating a remote information system terminal, whereby the host system disconnects the terminal and reestablishes contact.

Ca-Ce

Canister - Type of protective package used to contain and dispense keying material in punched or printed tape form.

Cascading - Downward flow of information through a range of security levels greater than the accreditation range of a system network or component.

Category - Restrictive label applied to classified or unclassified information to limit access.

Central Processing Unit (CPU) - The integrated circuit responsible for executing instructions, performing calculations and other data manipulations in a computer.

Central Services Node (CSN) – Is the Key Management Infrastructure core node that provides central security management and data management services.

Certificate - A digitally signed representation of information that:

- Identifies the authority issuing it;
- Identifies the subscriber;
- Identifies its valid operational period (date issued / expiration date).

Certificate management - Is the process whereby certificates (as defined above) are generated, stored, protected, transferred, loaded, used, and destroyed.

Certificate Policy (CP) - 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.

Certificate related information - Data, such as a subscriber's postal address that is not included in a certificate. This may be used by a Certification Authority (CA) in managing certificates.

Certificate Revocation List (CRL) - A list of revoked public key certificates created and digitally signed by a Certification Authority.

Certificate Status Authority (CSA) - 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.

Certification - Comprehensive evaluation of the technical and non-technical security safeguards of an information system to support the accreditation process that establishes the extent to which a particular design and implementation meets a set of specified security requirements.

Certification analyst - The independent technical liaison for all stakeholders involved in the C&A process responsible for objectively and independently evaluating a system as part of the risk management process. Based on the security requirements documented in the security plan, performs a technical and non-technical review of potential vulnerabilities in the system and determines if the security controls (management, operational, and technical) are correctly implemented and effective.

Certification authority (CA) - For Certification and Accreditation (C&A) (C&A Assessment): Official responsible for performing the comprehensive evaluation of the security features of an information system and determining the degree to which it meets its security requirements; For Public Key Infrastructure (PKI): A trusted third party that issues digital certificates and verifies the identity of the holder of the digital certificate.

Certification Authority Workstation (CAW) – Is a Commercial-off-the-shelf (COTS) workstation with a trusted operating system and special purpose application software that is used to issue certificates.

Certification package- Is a product of the certification effort documenting the detailed results of the certification activities.

Certification Practice Statement (CPS) - A listing 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); Software and hardware security tests conducted during development of an information system.

Certified TEMPEST Technical Authority (CTTA) - An experienced, technically qualified U.S. Government employee who has met established certification requirements in accordance with CNSS approved criteria and has been appointed by a U.S. Government Department or Agency to fulfill CTTA responsibilities.

Certifier - Individual responsible for making a technical judgment of the system's compliance with stated requirements, identifying and assessing the risks associated with operating the system, coordinating the certification activities, and consolidating the final certification and accreditation packages.

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.

Cha-Ci

Chain of evidence- Is a process and record that shows who obtained the evidence; where and when the evidence was obtained; who secured the evidence; and who had control or possession of the evidence. The "sequencing" of the chain of evidence follows this order: collection and identification; analysis; storage; preservation; presentation in court; return to owner.

Challenge and reply authentication - Prearranged procedure in which a subject requests authentication of another and the latter establishes validity with a correct reply.

Check word - Cipher text generated by cryptographic logic to detect failures in cryptography.

Checksum - Value computed on data to detect error or manipulation.

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 systems are 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 system 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.

> Note: Organizations subordinate to federal agencies may use the term Chief Information Officer to denote individuals filling positions with similar security responsibilities to agency-level Chief Information Officers.

Chief Information Security Officer (CISO) - See Senior Agency Information Security Officer.

Chunked-Encoding Transfer Attempt - The vulnerability is a buffer overflow in the chunked encoding transfer mechanism in the Internet Information Server Active pages. This vulnerability allows attackers to execute arbitrary code or to cause Denial of Service.

Cipher - Any cryptographic system in which arbitrary symbols or groups of symbols, represent units of plain text, or in which units of plain text are rearranged, or both.

Cipher text/ciphertext - Data in its encrypted form.

Cipher Text Auto-Key (CTAK) - Cryptographic logic that uses previous cipher text to generate a key stream.

Ciphony - Process of enciphering audio information, resulting in encrypted speech.

Cl

Claimant - An entity (user, device or process) whose assertion is to be verified using an authentication protocol.

Classified Information Spillage – Is a security incident that occurs whenever classified data is spilled either onto an unclassified information system or to an information system with a lower level of classification.

Clear Screen Policy - A policy that directs all computer users to ensure that the contents of the screen are protected from prying eyes and opportunistic breaches of confidentially. Typically, the easiest means of compliance is to use a screen saver that engages either on request or after a specified short period of time.

Clearance - Formal certification of authorization to have access to classified information other than that protected in a special access program (including SCI). Clearances are of three types: confidential, secret, and top secret. A top secret clearance permits access to top secret, secret, and confidential material; a secret clearance, to secret and confidential material; and a confidential clearance, to confidential material.

Clearing - Removal of data from an information system, its storage devices, and other peripheral devices with storage capacity, in such a way that the data may not be reconstructed using common system capabilities (i.e., through the keyboard); however, the data may be reconstructed using laboratory methods.

Client- Is an individual or process acting on behalf of an individual who makes requests of a guard or dedicated server. The client's requests to the guard or dedicated server can involve data transfer to, from, or through the guard or dedicated server.

Closed Security environment – Is an environment providing sufficient assurance that applications and equipment are protected against the introduction of malicious logic during an information system life cycle. Closed security is based upon a system's developers, operators, and maintenance personnel having sufficient clearances, authorization, and configuration control.

Closed storage - Storage of classified information within an accredited facility, in General Services Administration approved secure containers, while the facility is unoccupied by authorized personnel.

Cloud computing - A model for enabling on-demand network access to a shared pool of configurable IT capabilities/ resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. It allows users to access technology-based services from the network cloud without knowledge of, expertise with, or control over the technology infrastructure that supports them.

Co- Com

Code - System of communication in which arbitrary groups of letters, numbers, or symbols represent units of plain text of varying length; a term often used informally to describe software language.

Code book – Is a document containing plain text and code equivalents in a systematic arrangement or a technique of machine encryption using a word substitution technique.

Code group - Group of letters, numbers, or both in a code system used to represent a plain text word, phrase, or sentence.

Coder – A computer programmer or one who writes computer programming language code.

Code vocabulary - Set of plain text words, numerals, phrases, or sentences for which code equivalents are assigned in a code system.

Cold site – Is a backup site that can be up and operational in a relatively short time span, such as a day or two. Provision of services, such as telephone lines and power, is taken care of, and the basic office furniture might be in place, but there is unlikely to be any computer equipment, even though the building might well have a network infrastructure and a room ready to act as a server room. In most cases, cold sites provide the physical location and basic services.

Cold start – Is a procedure for initially keying crypto-equipment.

Command authority – Is an individual responsible for the appointment of user representatives for a department, agency, or organization and their key ordering privileges.

Common Access Card (CAC) - Standard identification/smart card issued by the Department of Defense that has an embedded integrated chip storing public key infrastructure (PKI) certificates.

Common control – Is a security control that is inherited by one or more organizational information systems. See Security Control Inheritanc

Common Criteria - Governing document that provides a comprehensive, rigorous method for specifying security function and assurance requirements for products and systems.

Common fill device - One of a family of devices developed to read-in, transfer, or store cryptographic key material.

Common Gateway Interface (CGI) - A set of rules that describe how a *Web Server* communicates with another piece of software on the same machine, and how the other piece of software (the CGI program) talks to the web server. Any piece of software can be a CGI program if it handles input and output according to the CGI standard.

Com

Common Vulnerabilities and Exposures (CVE) – Is a dictionary of common names for publicly known information system vulnerabilities.

Communications cover - Concealing or altering of characteristic communications patterns to hide information that could be of value to an adversary.

Communications deception – Is the deliberate transmission, retransmission, or alteration of communications to mislead an adversary's interpretation of the communications.

Communications profile - Analytic model of communications associated with an organization or activity. The model is prepared from a systematic examination of communications content and patterns, the functions they reflect, and the communications security measures applied.

Communications Security (COMSEC) - A component of Information Assurance that deals with measures and controls taken to deny unauthorized persons information derived from telecommunications and to ensure the authenticity of such telecommunications. COMSEC includes crypto security, transmission security, emissions security, and physical security of COMSEC material.

Community of Interest (COI) - A collaborative group of users who exchange information in pursuit of their shared goals, interests, missions, or business processes, and who therefore must have a shared vocabulary for the information they exchange. The group exchanges information within and between systems to include security domains.

Community risk - Probability that a particular vulnerability will be exploited within an interacting population and adversely impact some members of that population.

Compartmentalization - A nonhierarchical grouping of sensitive information used to control access to data more finely than with hierarchical security classification alone.

Compartmented mode - Mode of operation wherein each user with direct or indirect access to a system, its peripherals, remote terminals, or remote hosts has all of the following: 1) valid security clearance for the most restricted information processed in the system, 2) formal access approval and signed nondisclosure agreements for that information which a user is to have access, and 3) valid need-to-know for information which a user is to have access.

Compensating security control - A management, operational, and/or technical control (i.e., safeguard or countermeasure) employed by an organization in lieu of a recommended security control in the low, moderate, or high baselines that provides equivalent or comparable protection for an information system.

Comp

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.

Compromising emanations - Unintentional signals that, if intercepted and analyzed, would disclose the information transmitted, received, handled, or otherwise processed by information system equipment.

Computer abuse – Is an intentional or reckless misuse, alteration, disruption, or destruction of information processing resources.

Computer cryptography – Is the use of a crypto-algorithm program by a computer to authenticate or encrypt/decrypt information.

Computer Emergency Response Team (CERT) - An organization that studies computer and network information security in order to provide incident response services to victims of attacks, publish alerts concerning vulnerabilities and threats, and offer other information to help improve computer and network security.

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

Computer Incident Response Team (CIRT) - Group of individuals usually consisting of Security Analysts organized to develop, recommend, and coordinate immediate mitigation actions for containment, eradication, and recovery resulting from computer security incidents. It is also called a Computer Security Incident Response Team (CSIRT) or a CIRC (Computer Incident Response Center, Computer Incident Response Capability or Cyber Incident Response Team).

Computer Network Attack (CNA) - Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves; A category of fires employed for offensive purposes in which actions are taken through the use of computer networks to disrupt, deny, degrade manipulate or destroy information resident in the target information system or computer networks, or the systems/ networks themselves. The ultimate intended effect is not necessarily on the targeted system itself, but may support a larger effort, such as information operations or counter-terrorism

Computer Network Defense (CND) - Actions taken to defend against unauthorized activity within computer networks. CND includes monitoring, detection, analysis (such as trend and pattern analysis), and response and restoration activities.

Comp-Coms

Computer Network Exploitation (CNE) - Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary information systems or networks; Enabling Operations and intelligence collection capabilities conducted through the use of computer networks to gather data about target or adversary automated information systems or networks.

Computer Network Operations (CNO) - Comprised of computer network attack, computer network defense, and related computer network exploitation enabling operations.

Computer Security (COMPUSEC) - Measures and controls that ensure confidentiality, integrity, and availability of information system assets including hardware, software, firmware, and information being processed, stored, and communicated.

Computer security object - 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.

Computer security objects register - A collection of computer security object names and definitions kept by a registration authority.

Computer security subsystem - Hardware/software designed to provide computer security features in a larger system environment.

Computing environment – Is a workstation or server (host) and its operating system, peripherals, and applications.

COMSEC account - Administrative entity, identified by an account number, used to maintain accountability, custody, and control of COMSEC material.

COMSEC account audit - Examination of the holdings, records, and procedures of a COMSEC account ensuring all accountable COMSEC material is properly handled and safeguarded.

COMSEC aid – Is a COMSEC material that assists in securing telecommunications and is required in the production, operation, or maintenance of COMSEC systems and their components. COMSEC keying material, call sign/frequency systems, and supporting documentation, such as operating and maintenance manuals, are examples of COMSEC aids.

COMSEC assembly – Is a group of parts, elements, subassemblies, or circuits that are removable items of COMSEC equipment.

Coms

COMSEC boundary - Definable perimeter encompassing all hardware, firmware, and software components performing critical COMSEC functions, such as key generation, handling, and storage.

COMSEC control program - Computer instructions or routines controlling or affecting the externally performed functions of key generation, key distribution, message encryption/decryption, or authentication.

COMSEC custodian - Individual designated by proper authority to be responsible for the receipt, transfer, accounting, safeguarding, and destruction of COMSEC material assigned to a COMSEC account.

COMSEC demilitarization - Process of preparing COMSEC equipment for disposal by extracting all CCI, classified, or CRYPTO marked components for their secure destruction, as well as defacing and disposing of the remaining equipment hulk.

COMSEC element - Removable item of COMSEC equipment, assembly, or subassembly; normally consisting of a single piece or group of replaceable parts.

COMSEC end-item – Is the equipment or combination of components ready for use in a COMSEC application.

COMSEC equipment - Equipment designed to provide security to telecommunications by converting information to a form unintelligible to an unauthorized interceptor and, subsequently, by reconverting such information to its original form for authorized recipients; also, equipment designed specifically to aid in, or as an essential element of, the conversion process. COMSEC equipment includes cryptographic equipment, crypto-ancillary equipment, cryptographic production equipment, and authentication equipment.

COMSEC facility - Authorized and approved space used for generating, storing, repairing, or using COMSEC material.

COMSEC incident – Is the occurrence that potentially jeopardizes the security of COMSEC material or the secure electrical transmission of national security information or information governed by 10 U.S.C. Section 2315.

COMSEC insecurity - COMSEC incident that has been investigated, evaluated, and determined to jeopardize the security of COMSEC material or the secure transmission of information.

COMSEC manager – Is an individual who manages the COMSEC resources of an organization.

COMSEC material - Item designed to secure or authenticate telecommunications. COMSEC material includes, but is not limited to key, equipment, devices, documents, firmware, or software that embodies or describes cryptographic logic and other items that perform COMSEC functions.

COMSEC Material Control System (CMCS) - Logistics and accounting system through which COMSEC material marked "CRYPTO" is distributed, controlled, and safeguarded. Included are the COMSEC central offices of record, crypto logistic depots, and COMSEC accounts. COMSEC material other than key may be handled through the CMCS.

COMSEC modification – See: information systems security equipment modification.

COMSEC module - Removable component that performs COMSEC functions in a telecommunications equipment or system.

COMSEC monitoring - Act of listening to, copying, or recording transmissions of one's own official telecommunications to analyze the degree of security.

COMSEC profile - Statement of COMSEC measures and materials used to protect a given operation, system, or organization.

COMSEC survey – Is an organized collection of COMSEC and communications information relative to a given operation, system, or organization.

COMSEC system data - Information required by a COMSEC equipment or system to enable it to properly handle and control key.

COMSEC training - Teaching of skills relating to COMSEC accounting, use of COMSEC aids, or installation, use, maintenance, and repair of COMSEC equipment.

Confidentiality - The property that information is not disclosed to system entities (users, processes, devices) unless they have been authorized to access the information; Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Configuration control – Is the process of controlling modifications to hardware, firmware, software, and documentation to protect the information system against improper modifications prior to, during, and after system implementation.

Configuration Control Board (CCB) - A group of qualified people with responsibility for the process of regulating and approving changes to hardware, firmware, software, and documentation throughout the development and operational lifecycle of an information system.

Contamination - Type of incident involving the introduction of data of one security classification or security category into data of a lower security classification or different security category.

Contingency key - Key held for use under specific operational conditions or in support of specific contingency plans. See reserve keying material.

Cont

Contingency plan - Management policy and procedures used to guide an enterprise response to a perceived loss of mission capability. The Contingency Plan is the first plan used by the enterprise risk managers to determine what happened, why, and what to do. It may point to the COOP or Disaster Recovery Plan for major disruptions.

Continuity of Operations Plan (COOP) - Management policy and procedures used to guide an enterprise response to a major loss of enterprise capability or damage to its facilities. The COOP is the third plan needed by the enterprise risk managers and is used when the enterprise must recover (often at an alternate site) for a specified period of time. This also defines the activities of individual departments and agencies and their sub-components to ensure that their essential functions are performed. This includes plans and procedures that delineate essential functions; specifies succession to office and the emergency delegation of authority; provide for the safekeeping of vital records and databases; identify alternate operating facilities; provide for interoperable communications, and validate the capability through tests, training, and exercises.

Continuous monitoring - The process implemented to maintain a current security status for one or more information systems or for the entire suite of information systems on which the operational mission of the enterprise depends. The process includes: 1) The development of a strategy to regularly evaluate selected IA controls/metrics, 2) Recording and evaluating IA relevant events and the effectiveness of the enterprise in dealing with those events, 3) Recording changes to IA controls, or changes that affect IA risks, and 4) Publishing the current security status to enable information sharing decisions involving the enterprise.

Controlled access area - Physical area (e.g., building, room, etc.) to which only authorized personnel are granted unrestricted access. All other personnel are either escorted by authorized personnel or are under continuous surveillance.

Controlled access protection – Is a minimum set of security functionality that enforces access control on individual users and makes them accountable for their actions through login procedures, auditing of security-relevant events, and resource isolation.

Controlled area - Any area or space for which the organization has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting the information and/or information system.

Controlled Cryptographic Item (CCI) - Secure telecommunications or information system, or associated cryptographic component, that is unclassified and handled through the COMSEC Material Control System (CMCS), an equivalent material control system, or a combination of the two that provides accountability and visibility. Such items are marked "Controlled Cryptographic Item", or, where space is limited, "CCI".

Controlled Cryptographic Item (CCI) assembly – Is a device embodying a cryptographic logic or other COMSEC design that NSA has approved as a Controlled Cryptographic Item (CCI). It performs the entire COMSEC function, but depends upon the host equipment to operate.

Controlled Cryptographic Item (CCI) component - Part of a Controlled Cryptographic Item (CCI) that does not perform the entire COMSEC function but depends upon the host equipment, or assembly, to complete and operate the COMSEC function.

Controlled Cryptographic Item (CCI) equipment – Is a telecommunications or information handling equipment that embodies a Controlled Cryptographic Item (CCI) component or CCI assembly and performs the entire COMSEC function without dependence on host equipment to operate.

Controlled interface – Is a boundary with a set of mechanisms that enforces the security policies and controls the flow of information between interconnected information systems.

Controlled space - Three-dimensional space surrounding information system equipment, within which unauthorized individuals are denied unrestricted access and are either escorted by authorized individuals or are under continuous physical or electronic surveillance.

Controlling authority - Official responsible for directing the operation of a cryptonet and for managing the operational use and control of keying material assigned to the cryptonet.

Cookie - Data exchanged between an HTTP server and a browser (a client of the server) to store state information on the client side and retrieve it later for server use.

Cookie - A small file that is downloaded by some websites to store a packet of information on your browser. Companies and organizations use cookies to remember your login or registration identification, site preferences, pages viewed and online "shopping-cart" so that the next time you visit a site, your stored information can automatically be pulled up for you.

Cooperative key generation - Electronically exchanging functions of locally generated, random components, from which both terminals of a secure circuit construct traffic encryption key or key encryption key for use on that circuit.

Cooperative remote rekeying - Synonymous with: manual remote rekeying.

Correctness proof – Is a mathematical proof of consistency between a specification and its implementation.

Counter Cyber (CC) - A mission that integrates offensive and defensive operations to attain and maintain a desired degree of cyberspace superiority. Counter-cyber missions are designed to disrupt, negate, and/ or destroy adversarial cyberspace activities and capabilities, both before and after their employment

Cou-Cr

Countermeasure - Actions, devices, procedures, or techniques that meet or oppose(i.e., counters) a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken; Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system.

Covert channel – Is an unauthorized communication path that manipulates a communications medium in an unexpected, unconventional or unforeseen way in order to transmit information without detection by anyone other than the entities operating the covert channel.

Covert channel analysis - Determination of the extent to which the security policy model and subsequent lower-level program descriptions may allow unauthorized access to information.

Covert storage channel – is a covert channel involving the direct or indirect writing to a storage location by one process and the direct or indirect reading of the storage location by another process. Covert storage channels typically involve a finite resource (e.g., sectors on a disk) that is shared by two subjects at different security levels.

Covert timing channel – Is a covert channel in which one process signals information to another process by modulating its own use of system resources (e.g., central processing unit time) in such a way that this manipulation affects the real response time observed by the second process.

Credential - Evidence or testimonials that support a claim of identity or assertion of an attribute and usually are intended to be used more than once.

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.

Critical infrastructure - Critical infrastructure are the assets, systems, and networks, whether physical or virtual, so vital to the state that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

- **SAMPLES OF CRITICAL INFRASTRUCTURE**
  - Communications, Dams, Energy, Financial Services (Banks), Government Facilities, Healthcare, and Publix Health, Information Technology, Transportation Systems, Water, Waste water System

Critical security parameter – Is 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.

Criticality level - Refers to the (consequences of) incorrect behavior of a system. The more serious the expected direct and indirect effects of the incorrect behavior, the higher the criticality level.

Cross certificate - A certificate issued from a CA that signs the public key of another CA not within its trust hierarchy that establishes a trust relationship between the two CAs. A certificate used to establish a trust relationship between two Certification Authorities.

Cross domain capabilities - The set of functions that enable the transfer of information between security domains in accordance with the policies of the security domains involved.

Cross Domain Solution (CDS)- A form of controlled interface that provides the ability to manually and/or automatically access and/or transfer information between different security domains.

Cross-site Scripting (XSS)- An attack that uses third-party web resources to run script within the victim's web browser or application. This occurs when a browser visits a malicious website or clicks on a malicious link.

Cryptanalysis- Operations performed in defeating encryption without an initial knowledge of the key employed in providing the protection (also known as Cryptographic Analysis). Operations performed in defeating cryptographic protection without an initial knowledge of the key employed in providing the protection; the study of mathematical techniques for attempting to defeat cryptographic techniques and/or information systems security. This includes the process of looking for errors or weaknesses in the implementation of an algorithm or of the algorithm itself.

Cryptographic - Pertaining to, or concerned with, cryptography.

Cryptographic alarm – Is a circuit or device that detects failures or aberrations in the logic or operation of cryptographic equipment. Crypto-alarm may inhibit transmission or may provide a visible and/or audible alarm.

Cryptographic algorithm – Is a well-defined computational procedure that takes variable inputs, including a cryptographic key, and produces an output.

Cryptographic ancillary equipment - Equipment designed specifically to facilitate efficient or reliable operation of cryptographic equipment, without performing cryptographic functions itself.

Cryptographic binding - Associates two or more related elements of information using cryptographic techniques.

Cryp

Cryptographic component – Is a hardware or firmware embodiment of the cryptographic logic. A cryptographic component may be a modular assembly, a printed wiring assembly, a microcircuit, or a combination of these items.

Cryptographic equipment – Is equipment that embodies a cryptographic logic.

Cryptographic Ignition Key (CIK) - Device or electronic key used to unlock the secure mode of cryptographic equipment.

Cryptographic initialization - Function used to set the state of a cryptographic logic prior to key generation, encryption, or other operating mode.

Cryptographic logic - The embodiment of one (or more) cryptographic algorithm(s) along with alarms, checks, and other processes essential to effective and secure performance of the cryptographic processes.

Cryptographic material (“crypto”**) -** COMSEC material used to secure or authenticate information.

Cryptographic net - Stations holding a common key.

Cryptographic period – Is the time span during which each key setting remains in effect.

Cryptographic product - A cryptographic key (public, private, or shared) or public key certificate, used for encryption, decryption, digital signature, or signature verification; and other items, such as compromised key lists (CKL) and certificate revocation lists (CRL), obtained by trusted means from the same source which validate the authenticity of keys or certificates. Protected software which generates or regenerates keys or certificates may also be considered a cryptographic product.

Cryptographic randomization - Function that randomly determines the transmit state of a cryptographic logic.

Cryptographic security – Is a component of COMSEC resulting from the provision of technically sound cryptographic systems and their proper use.

Cryptographic synchronization – Is a process by which a receiving decrypting cryptographic logic attains the same internal state as the transmitting encrypting logic.

Cryptographic system - Associated information assurance items interacting to provide a single means of encryption or decryption.

Cryptographic system analysis - Process of establishing the exploitability of a cryptographic system, normally by reviewing transmitted traffic protected or secured by the system under study.

Cryptographic system evaluation – Is the process of determining vulnerabilities of a cryptographic system and recommending countermeasures.

Cryptographic system review – Is examination of a cryptographic system by the controlling authority ensuring its adequacy of design and content, continued need, and proper distribution.

Cryptographic system survey – Is a management technique in which actual holders of a cryptographic system express opinions on the system's suitability and provide usage information for technical evaluations.

Cryptographic token - A portable, user-controlled, physical device (e.g., smart card or PCMCIA card) used to store cryptographic information and possibly also perform cryptographic functions.

Cryptography - Art or science concerning the principles, means, and methods for rendering plain information unintelligible and for restoring encrypted information to intelligible form.

Cryptology - The mathematical science that deals with cryptanalysis and cryptography.

Cyber - Term used synonymously with "information technology" or "computer". It is often used in conjunction with another word or phrase to form a compound subject, such as "cyber security" or "cyber terrorism."

Cyber attack – Is an attack via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information; A hostile act using computer or related networks or systems, and intended to disrupt and/ or destroy an adversary's critical cyber systems, assets, or functions

Cyber bullying - Any form of harassment, threat, or humiliation done through the internet or other communication devices which are deliberately aimed at another person

Cybercrime - Criminal activities carried out through the use of information and communication networks, especially the internet

Cyber defense - The integrated application of DoD on cyberspace capabilities and processes to synchronize in real-time the ability to detect, analyze and mitigate threats and vulnerabilities, and outmaneuver adversaries, in order to defend designated networks, protect critical missions, and enable US freedom of action.

Cyber Defense includes:

- Proactive NetOps: (e.g., configuration control, information assurance (IA) measures, physical security and secure architecture design, intrusion detection, firewalls, signature updates, encryption of data at rest);
- Defensive Counter Cyber (DCC): Includes: military deception via honeypots and other operations; and redirection, deactivation, or removal of malware engaged in a hostile act/ imminent hostile act.
- Defensive Countermeasures.

Cyber espionage - the act or practice of obtaining secrets (sensitive, proprietary or classified information) from individuals, competitors, rivals, groups, governments and enemies also for military, political, or economic advantage using illegal exploitation methods on internet, networks, software and or computers. Classified information that is not handled securely can be intercepted and even modified, making espionage possible from the other side of the world.

Cyber incident - Actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein.

Cyber operation - The employment of cyber capabilities with the primary purpose of achieving objectives in or by the use of cyberspace

Cybersecurity - The ability to protect or defend the use of cyberspace from cyber-attacks. The collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment, organization and users' assets.

General security objectives:

- Availability;
  This is the capability of the system to protect data and processes from the denial of service to the authorized users.

Main threat: Distributed Denial of Service.

- Integrity (which may include authenticity and non-repudiation); the capability of the system to protect data and processes from unauthorized changes.

Main threats: Exploit, Rootkit.

- Confidentiality.
  This is the capability of the system to protect data and processes from unauthorized access.

Main threats: Eavesdropping, Key logging, Data Exfiltration.

Cybersecurity Policy - Constitutes strategies and standards regarding the security of operations in cyberspace, and encompasses the full range of threat and vulnerability reduction, deterrence, international engagement, incident responses, resiliency, and recovery policies and activities

Cyber terrorism - Is the use of information technology for attacks or threats by terrorist organizations. The broadest definition, created by Kevin Coleman of the Technolytics Institute, classifies cyber terrorism as "the premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or further social, ideological, religious, political, or similar objectives or to intimidate any person in the furtherance of such objectives. Is any premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by subnational groups or clandestine agents. A cyber terrorist attack is designed to cause physical harm or extreme financial harm.

Cyber war - any cyber attack that causes widespread harm is cyber war, though that begs the question of what constitutes harm—psychological, economic, or physical threats; The use of computers to disrupt activities of an enemy country, especially the deliberate attacking of communication systems and networks.

Cyber warfare - Cyber warfare only if they take place alongside actual military operations; Is any virtual conflict initiated as a politically motivated attack on an enemy's computer and information systems. Waged via the internet, these attacks disable financial and organizational systems by stealing or altering classified data to undermine networks, websites and services.

CHARACTERISTICS OF CYBER WARFARE:

- Anonymous
- Little cost and resources
- Attacks can be perpetrated by the few upon the many
- Launched from any billions of sources worldwide
- Impacts immediate and obvious, dormant and subtle
- Degree of damage range from inconvenient downtime to life threatening destructions of critical infrastructures to government and state paralysis.

Cybercrime offense - Offenses against the confidentiality, integrity, and availability of computer data and systems

Cyberspace - An interactive domain made up of digital networks that are used to store, modify and communicate information. It includes the internet, but also the other information systems that support our businesses, infrastructure and services. A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers; A global domain within the virtual information environment consisting of the interdependent network of information technology infrastructures including the internet, telecommunications networks, computer systems and embedded processors and control.

Cyber-squatting - The acquisition of a domain name over the internet in bad faith to profit, mislead, destroy reputation, and deprive others from registering the same domain name

Cyclic redundancy check - Error checking mechanism that verifies data integrity by computing a polynomial algorithm based checksum.

D

Data - A subset of information in an electronic format that allows it to be retrieved or transmitted.

Data aggregation – Is a compilation of individual data systems and data that could result in the totality of the information being classified, or classified at a higher level, or of beneficial use to an adversary.

Da-De

Data asset – Is any entity that is comprised of data. For example, a database is a data asset that is comprised of data records. A data asset may be a system or application output file, database, document, or web page. A data asset also includes a service that may be provided to access data from an application. For example, a service that returns individual records from a database would be a data asset. Similarly, a web site that returns data in response to specific queries (e.g., www.weather.com) would be a data asset.

Data Base - A database is a collection of data records. On web databases, records may consist of web pages, graphics, audio files, newspaper files, books, movies or anything from very general to very specific areas of interest. Database records are usually indexed and come with a search interface to find records of interest.

Data element – Is 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.

Data flow control - Synonymous with information flow control.

Data integrity - The property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner.

Data origin authentication - The process of verifying that the source of the data is as claimed and that the data has not been modified.

Data security– Is the protection of data from unauthorized (accidental or intentional) modification, destruction, or disclosure. See also information security.

Data transfer device (DTD) - Fill device designed to securely store, transport, and transfer electronically both COMSEC and TRANSEC key, designed to be backward compatible with the previous generation of COMSEC common fill devices, and programmable to support modern mission systems.

Data Warehousing – Is the consolidation of several previously independent databases into one location.

Decertification - Revocation of the certification of an information system item or equipment for cause.

Decipher - Convert enciphered text to plain text by means of a cryptographic system.

Decode - Convert encoded text to plain text by means of a code.

Decrypt - Generic term encompassing decode and decipher.

De

Dedicated mode- Information systems security mode of operation wherein each user, with direct or indirect access to the system, its peripherals, remote terminals, or remote hosts, has all of the following:

1. valid security clearance for all information within the system,
2. formal access approval and signed nondisclosure agreements for all the information stored and/or processed (including all compartments, sub compartments, and/or special access programs), and
3. Valid need-to-know for all information contained within the information system. When in the dedicated security mode, a system is specifically and exclusively dedicated to and controlled for the processing of one particular type or classification of information, either for full-time operation or for a specified period of time.

Default classification - Classification reflecting the highest classification being processed in an information system. Default classification is included in the caution statement affixed to an object.

Defense-in-Breadth - A planned, systematic set of multi-disciplinary activities that seek to identify, manage, and reduce risk of exploitable vulnerabilities at every stage of the system, network, or sub-component lifecycle (system, network, or product design and development; manufacturing; packaging; assembly; system integration; distribution; operations; maintenance; and retirement).

Defense-in-Depth - Information Security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization.

Defense-in-depth - Defense in depth is the concept of protecting a computer network with a series of defensive mechanisms such that if one mechanism fails, another will already be in place to thwart an attack.

Degauss - Procedure to reduce the magnetic flux to virtual zero by applying a reverse magnetizing field; also called demagnetizing.

Delegated development program- INFOSEC program in which the Director, NSA, delegates, on a case-by-case basis, the development and/or production of an entire telecommunications product, including the INFOSEC portion, to a lead department or agency.

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.

Delivery-Only Client (DOC) - A configuration of a client node that enables a DOA agent to access a primary services node (PRSN) to retrieve KMI products and access KMI services. A DOC consists of a client platform but does not include an AKP.

Demilitarized Zone (DMZ) - Perimeter network segment that is logically between internal and external networks. Its purpose is to enforce the internal network's Information Assurance policy for external information exchange and to provide external, untrusted sources with restricted access to releasable information while shielding the internal networks from outside attacks.

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.)

Denial of Service (DoS) Attack - The prevention of authorized access to a system resource or the delaying of system operations and functions. Often this involves a cyber criminal "flooding" a system with more information requests than the web server can handle. See also Distributed Denial of Service (DDos) Attack.

Descriptive Top-Level Specification (DTLS) – Is a natural language descriptive of a system's security requirements, an informal design notation, or a combination of the two.

Designated Approval Authority (DAA) - Official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. This term is synonymous with authorizing official, designated accrediting authority, and delegated accrediting authority.

Destination Unreachable Host Unreachable - If the IP module cannot deliver the datagram because the indicated protocol module or process port is not active, the destination host may send a destination unreachable message to the source hose – it is a message which a user would usually get from the remote gateway when the destination host is unreachable.

Device distribution profile – Is an approval-based Access Control List (ACL) for a specific product that 1) names the user devices in a specific KMI Operating Account (KOA) to which primary services node s (PRSNs) distribute the product and 2) states conditions of distribution for each device.

Device registration manager – Is the management role that is responsible for performing activities related to registering users that are devices.

Dial back- Synonymous with call back.

Dictionary Attack – Is a password-cracking attack that tries all of the phrases or words in a dictionary.

Digital Certificate – Is the electronic equivalent of an ID card that establishes your credentials when doing business or other transactions on the Web.

Digital signature - Cryptographic process used to assure data object originator authenticity, data integrity, and time stamping for prevention of replay.

Digital Subscriber Line (DSL) - A method for moving data over regular phone lines. A DSL circuit is much faster than a regular phone connection, and the wires coming into the subscriber's premises are the same (copper) wires used for regular phone service. A DSL circuit must be configured to connect two specific locations, similar to a leased line (however a DSL circuit is not a *leased line*. A common configuration of DSL allows downloads at speeds of up to 1.544 megabits (not megabytes) per second, and uploads at speeds of 128 kilobits per second. This arrangement is called *ADSL*: Asymmetric Digital Subscriber Line. Another common configuration is symmetrical: 384 Kilobits per second in both directions.

Disaster Recovery Plan (DRP) - Management policy and procedures used to guide an enterprise response to a major loss of enterprise capability or damage to its facilities. The DRP is the second plan needed by the enterprise risk managers and is used when the enterprise must recover (at its original facilities) from a loss of capability over a period of hours or days. See Continuity of Operations Plan and Contingency Plan.

Discretionary Access Control (DAC) - A means of restricting access to objects (e.g., files, data entities) based on the identity and need-to-know of subjects (e.g., users, processes) and/or groups to which the object belongs. The controls are discretionary in the sense that a subject with certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject (unless restrained by mandatory access control).

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).

Distinguished Name (DN) - A unique name or character string that unambiguously identifies an entity according to the hierarchical naming conventions of X.500 directory service.

Distinguishing identifier – Is information which unambiguously distinguishes an entity in the authentication process.

Distributed Denial of Service (DDos) - A Denial of Service technique that uses numerous hosts to perform the attack; A class of attacks that results in the exhaustion of computing or communications resources by engaging many intermediate computers to simultaneously attack one victim. These intermediate attack systems are often previously compromised and under the control of the attacker.

Distributed Denial of Service (DDos) Attack – Is a variant of the denial of service attack that uses numerous hosts to perform the attack.

Domain - An environment or context that includes a set of system resources and a set of system entities that have the right to access the resources as defined by a common security policy, security model, or security architecture.

Domain Hijacking – Is an attack by which the attacker takes over a domain by first blocking access to the domain's DNS server and then putting his own server up in its place.

Domain Name - The conceptual system, standards, and names in the internet that make up the hierarchical organization of the Internet into named domains.

Domain Name System (DNS) - The Domain Name System (DNS) helps users to find their way around the Internet. Every computer on the Internet has a unique IP (Internet Protocol) address - just like a telephone number which is a rather complicated string of numbers. The DNS makes using the Internet easier by allowing a familiar string of letters (i.e. www.google.com) to be used instead of the arcane IP address (i.e. 74.125.224.72).

Drop accountability - Procedure under which a COMSEC account custodian initially receipts for COMSEC material, and provides no further accounting for it to its central office of record. Local accountability of the COMSEC material may continue to be required. See accounting legend code.

Dumpster Diving - A method of obtaining passwords and corporate directories or other sensitive data by searching through discarded media.

Dynamic Host Configuration Protocol (DHCP) - DHCP is a *protocol* by which a machine can obtain an *IP number* (and other network configuration information) from a *server* on the local *network*.

Dynamic Hypertext Markup Language (DHTML) - DHTML refers to *web pages* that use a combination of *HTML*, *JavaScript*, and *CSS* to create features such as letting the user drag items around on the web page, some simple kinds of animation, and many more.

E

Electronic authentication (e-authentication) - The process of establishing confidence in user identities electronically presented to an information system.

Electronic business (e-business) – Is doing business online.

Electronic Countermeasure - That division of Electronic Warfare involving actions taken to prevent or reduce an enemy's effective use of the electromagnetic spectrum, through the use of electromagnetic energy. There are three sub-divisions of ECM: Electronic Jamming, Electronic Deception and Electronic Neutralization.

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

Electronic Key Management System (EKMS) - Interoperable collection of systems being developed by services and agencies of the U.S. Government to automate the planning, ordering, generating, distributing, storing, filling, using, and destroying of electronic key and management of other types of COMSEC material.

Electronic messaging services - Services providing interpersonal messaging capability; meeting specific functional, management, and technical requirements; and yielding a business-quality electronic mail service suitable for the conduct of official government business.

Electronic signature – Is the process of applying any mark in electronic form with the intent to sign a data object. See also digital signature.

Electronic Warfare (EW) – Is any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. The three major subdivisions within electronic warfare are: electronic attack, electronic protection, and electronic warfare support.

Electronic Warfare – Is any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. The three major subdivisions within electronic warfare are: electronic attack, electronic protection, and electronic warfare support.

Electronically generated key - Key generated in a COMSEC device by introducing (either mechanically or electronically) a seed key into the device and then using the seed, together with a software algorithm stored in the device, to produce the desired key.

Emanations security (EMSEC) - Protection resulting from measures taken to deny unauthorized individuals information derived from intercept and analysis of compromising emissions from crypto-equipment or an information system.

Embedded computer- Is a computer system that is an integral part of a larger system.

Embedded cryptographic system- a Cryptosystem performing or controlling a function as an integral element of a larger system or subsystem.

Embedded cryptography- Cryptography engineered into equipment or system whose basic function is not cryptographic.

Encipher - Convert plain text to cipher text by means of a cryptographic system.

Enclave - Collection of information systems connected by one or more internal networks under the control of a single authority and security policy. The systems may be structured by physical proximity or by function, independent of location.

Enclave boundary - Point at which an enclave's internal network service layer connects to an external network's service layer, i.e., to another enclave or to a Wide Area Network (WAN).

Encode - Convert plain text to cipher text by means of a code.

Encrypt- Generic term encompassing enciphers and encode.

Enc-Ent

Encryption - The process of changing plaintext into ciphertext for the purpose of security or privacy. A data security technique used to protect information from unauthorized inspection or alteration. Information is encoded so that it appears as a meaningless string of letters and symbols during delivery or transmission. Upon receipt, the information is decoded using an encryption key.

Encryption algorithm - Set of mathematically expressed rules for rendering data unintelligible by executing a series of conversions controlled by a key.

Encryption certificate – Is a certificate containing a public key that can encrypt or decrypt electronic messages, files, documents, or data transmissions, or establish or exchange a session key for these same purposes. Key management sometimes refers to the process of storing protecting and escrowing

End Cryptographic Unit (ECU) - Device that 1) performs cryptographic functions, 2) typically is part of a larger system for which the device provides security services, and 3) from the viewpoint of a supporting security infrastructure (e.g., a key management system) is the lowest level of identifiable component with which a management transaction can be conducted.

End-item accounting – a counting for all the accountable components of a COMSEC equipment configuration by a single short title.

End-to-end encryption – is an encryption of information at its origin and decryption at its intended destination without intermediate decryption.

End-to-end security – is safeguarding information in an information system from point of origin to point of destination.

Enrollment manager – is the management role that is responsible for assigning user identities to management and non-management roles.

Enterprise - An organization with a defined mission/goal and a defined boundary, using information systems to execute that mission, and with responsibility for managing its own risks and performance.

Enterprise Architecture (EA) - The description of an enterprise's entire set of information systems: how they are configured, how they are integrated, how they interface to the external environment at the enterprise's boundary, how they are operated to support the enterprise mission, and how they contribute to the enterprise's overall security posture.

Enterprise risk management - The methods and processes used by an enterprise to manage risks to its mission and to establish the trust necessary for the enterprise to support shared missions. It involves the identification of mission dependencies on enterprise capabilities, the identification and prioritization of risks due to defined threats, the implementation of countermeasures to provide both a static risk posture and an effective dynamic response to active threats;

Enterprise service - A set of one or more computer applications and middleware systems hosted on computer hardware that provides standard information systems capabilities to end users and hosted mission applications and services.

Entrapment- Deliberate planting of apparent flaws in an information system for the purpose of detecting attempted penetrations.

Environment- An aggregate of external procedures, conditions, and objects affecting the development, operation, and maintenance of an information system.

Erasure - Process intended to render magnetically stored information irretrievable by normal means.

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.

Ethernet - A very common method of networking computers in a *LAN*. There is more than one type of Ethernet. By 2001 the standard type was "100-BaseT" which can handle up to about 100,000,000 bits-per-second and can be used with almost any kind of computer.

Evaluated Products List (EPL) - List of validated products that have been successfully evaluated under the National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS).

Evaluation Assurance Level (EAL) - Set of assurance requirements that represent a point on the Common Criteria predefined assurance scale.

Event - Any observable occurrence in a system and/or network. Events sometimes provide indication that an incident is occurring.

Exercise key- Cryptographic key material used exclusively to safeguard communications transmitted over-the-air during military or organized civil training exercises.

Exploit - A piece of software, a chunk of data, or sequence of commands that take advantage of a bug, glitch or vulnerability in order to cause unintended or unanticipated behavior to occur on computer software, hardware, or something electronic.

Exploitable channel – Is a channel that allows the violation of the security policy governing an information system and is usable or detectable by subjects external to the trusted computing base.

External information system (or component) - An information system or component of an information system that is outside of the authorization boundary established by the organization and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness.

External information system service - An information system service that is implemented outside of the authorization boundary of the organizational information system (i.e., a service that is used by, but not a part of, the organizational information system) and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness.

External network - A network not controlled by the organization.

Extraction resistance- Capability of crypto-equipment or secure telecommunications equipment to resist efforts to extract key.

Extranet – Is a private network that uses Web technology, permitting the sharing of portions of an enterprise's information or operations with suppliers, vendors, partners, customers, or other enterprises.

F

Failed State - A failed state is a state perceived as having failed at some of the basic conditions and responsibilities of a sovereign government. There is no general consensus on the definition of a failed state. The definition of a failed state according to the Fund for Peace is often used to characterize a failed state:

- loss of control of its territory, or of the monopoly on the legitimate use of physical force therein;
- erosion of legitimate authority to make collective decisions
- an inability to provide public services an inability to interact with other states as a full member of the international community

Failover – Is the capability to switch over automatically (typically without human intervention or warning) to a redundant or standby information system upon the failure or abnormal termination of the previously active system.

Fail safe - Automatic protection of programs and/or processing systems when hardware or software failure is detected.

Fail soft - Selective termination of affected nonessential processing when hardware or software failure is determined to be imminent.

Failure access - Type of incident in which unauthorized access to data results from hardware or software failure.

Failure control - Methodology used to detect imminent hardware or software failure and provide fail safe or fail soft recovery.

False acceptance - In biometrics: the instance of a security system incorrectly verifying or identifying an unauthorized person. It typically is considered the most serious of biometric security errors as it gives unauthorized users access to systems that expressly are trying to keep them out.

False Acceptance Rate (FAR) - The measure of the likelihood that the biometric security system will incorrectly accept an access attempt by an unauthorized user. A system's false acceptance rate typically is stated as the ratio of the number of false acceptances divided by the number of identification attempts.

False rejection - In biometrics: the instance of a security system failing to verify or identify an authorized person. It does not necessarily indicate a flaw in the biometric system; for example, in a fingerprint-based system, an incorrectly aligned finger on the scanner or dirt on the scanner can result in the scanner misreading the fingerprint, causing a false rejection of the authorized user.

False Rejection Rate (FRR) - The measure of the likelihood that the biometric security system will incorrectly reject an access attempt by an authorized user. A system's false rejection rate typically is stated as the ratio of the number of false rejections divided by the number of identification attempts.

Fault Line Attack - A Fault Line Attack uses weaknesses between interfaces of systems to exploit gaps in coverage.

Fiber Distributed Data Interface (FDDI) - A standard for transmitting data on optical fiber cables at a rate of around 100,000,000 bits-per-second (10 times as fast as 10-Base*TEthernet*, about twice as fast as *T-3*).

File protection - Aggregate of processes and procedures designed to inhibit unauthorized access, contamination, elimination, modification, or destruction of a file or any of its contents.

File security- Means by which access to computer files is only limited to authorized users.

File Transfer Protocol (FTP) - A standard Internet protocol implemented in FTP server and client software, including most web browsers. It is used to "transfer data reliably and efficiently. A very common method of moving files between two Internet sites.

Fill device - COMSEC item used to transfer or store key in electronic form or to insert key into cryptographic equipment.

Filter - Filters manage access to online content. A filter can restrict times when the internet can be accessed and also restrict what is viewed and downloaded based on certain key words or types of content. Some filters can also be instructed to specifically block information from being displayed. Types of filters range from those on home computers to filters used by a school on its server.

Firefly - Key management protocol based on public key cryptography.

Firewall - A hardware/software capability that limits access between networks and/or systems in accordance with a specific security policy; A hardware or software link in a network that inspects all data packets coming and going from a computer, permitting only those that are authorized to reach the other side.

Fir-Fr

Firmware - Computer programs and data stored in hardware - typically in read-only memory (ROM) or programmable read-only memory (PROM) - such that the programs and data cannot be dynamically written or modified during execution of the programs.

Fixed COMSEC facility - COMSEC facility located in an immobile structure or aboard a ship.

Flagging - Flagging is reporting content you encounter online because you believe it is inappropriate – for example, you may 'flag' a post on an online forum for moderators to review.

Flaw- An error of commission, omission, or oversight in an information system that may allow protection mechanisms to be bypassed.

Flaw hypothesis methodology- Is a system analysis and penetration technique in which the specification and documentation for an information system are analyzed to produce a list of hypothetical flaws. This list is prioritized on the basis of the estimated probability that a flaw exists, on the ease of exploiting it, and on the extent of control or compromise it would provide. The prioritized list is used to perform penetration testing of a system.

Flooding - An attack that attempts to cause a failure in a system by providing more input than the system can process properly.

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.

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

Formal access approval - A formalization of the security determination for authorizing access to a specific type of classified or sensitive information, based on specified access requirements, a determination of the individual's security eligibility and a determination that the individual's official duties require the individual be provided access to the information.

Formal development methodology- Is a software development strategy that proves security methodology design specifications.

Formal method- Is a mathematical argument which verifies that the system satisfies a mathematically described security policy.

Formal security policy- Is a mathematically precise statement of a security policy.

Frequency hopping – The repeated switching of frequencies during radio transmission according to a specified algorithm, to minimize unauthorized interception or jamming of telecommunications.

Full maintenance- Complete diagnostic repair, modification, and overhaul of COMSEC equipment, including repair of defective assemblies by piece part replacement. See limited maintenance.

Functional testing- Segment of security testing in which advertised security mechanisms of an information system are tested under operational conditions.

G

Gateway - A network point that acts as an entrance to another network.

General Support Systems (GSS) - An interconnected set of information resources under the same direct management control which shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people. A system can be, for example, a local area network (LAN) including smart terminals that supports a branch office, an agency-wide backbone, a communications network, a departmental data processing center including its operating system and utilities, a tactical radio network, or a shared information processing service organization (IPSO).

Global Information Grid (GIG) - The globally interconnected, end-to-end set of information capabilities for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and National Security Systems. Non-GIG IT includes stand-alone, self-contained, or embedded IT that is not, and will not be, connected to the enterprise network.

Global Information Infrastructure (GII) - Worldwide interconnections of the information systems of all countries, international and multinational organizations, and international commercial communications.

Gopher - Invented at the University of Minnesota in 1993 just before the *Web*, gopher was a widely successful method of making menus of material available over the Internet. Gopher was designed to be much easier to use than *FTP*, while still using a text-only interface. Gopher is a *Client* and *Server* style program, which requires that the user have a Gopher *Client* program. Although Gopher spread rapidly across the globe in only a couple of years, it has been largely supplanted by Hypertext, also known as *WWW (World Wide Web)*. There are still thousands of Gopher *Servers* on the Internet and we can expect they will remain for a while.

Group authenticator – Is used, sometimes in addition to a sign-on authenticator, to allow access to specific data or functions that may be shared by all members of a particular group.

Guard – Is a mechanism limiting the exchange of information between information systems or subsystems.

H

Hacker - Unauthorized user who attempts to or gains access to an information system; an individual who uses computer technology in ways not originally intended by the vendor. Commonly the term is applied to people who attack others using computers. For the purposes of this discussion, hackers are subdivided as follows:

- Script kiddies: Unskilled attackers who do not have the ability to discover new vulnerabilities or write exploit code, and are dependent on the research and tools from others. Their goal is achievement. Their sub-goals are to gain access and deface web pages.
- Worm and virus writers: Attackers who write the propagation code used in the worms and viruses but not typically the exploit code used to penetrate the systems infected. Their goal is notoriety. Their sub-goals are to cause disruption of networks and attached computer systems.
- Security researchers and white hat operators: This group has two subcategories:
    - bug hunters and exploit coders. Their goal is profit. Their subgoals are to improve security and achieve recognition with an exploit.
    - Professional hacker-black hat: Individuals who get paid to write exploits or actually penetrate networks; this group also falls into the same two subcategories as above. Their goal is also profit.

Hacker - An individual who attempts to break into a computer without authorization.

Hacktivism – Is a computer hacking intended to communicate a social or political message, or to support the position of a political or ideological group. Hacktivism activities include data theft, website defacement, denial of service, redirects and others; "hacktivism," perpetrated out of patriotism by anonymous citizens. Even if these attacks could be traced to government computers, it would not be solid proof.

Hacktivist – Is an attacker who practices hacktivism; a hacker who attacks information systems with the intent to advance a particular social or political agenda (i.e. Anonymous, LulzSec).

Handshaking procedures - Dialogue process between two information systems for synchronizing, identifying, and authenticating themselves to one another.

Hard copy key - Physical keying material, such as printed key lists, punched or printed key tapes, or programmable, read-only memories (PROM).

Hardware - The physical components of an information system.

Hardwired key – Is permanently installed key.

Hash total- Value computed on data to detect error or manipulation.

Hash-Based Message Authentication Code (HMAC) - A message authentication code that uses a cryptographic key in conjunction with a hash function.

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

Hashword- Memory address containing hash total.

High assurance guard- A guard that has two basic functional capabilities: a Message Guard and a Directory Guard. The Message Guard provides filter service for message traffic traversing the Guard between adjacent security domains. The Director Guard provides filter service for directory access and updates traversing the Guard between adjacent security domains.

High impact - The loss of confidentiality, integrity, or availability that could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, individuals, other organizations, or the national security interests of the United States; (i.e., 1) causes a severe degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; 2) results in major damage to organizational assets; 3) results in major financial loss; or 4) results in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.)

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

Hijack Attack - A form of active wiretapping in which the attacker seizes control of a previously established communication association.

Honeypot - A system (e.g., a web server) or system resource (e.g., a file on a server) that is designed to be attractive to potential crackers and intruders and has no authorized users other than its administrators.

Host - Any computer on a *network* that is a repository for services available to other computers on the *network*. It is quite common to have one host machine provide several services, such as *SMTP* (email) and *HTTP* (web).

Host - Any computer that has full two-way access to other computers.

Hot site - Backup site that includes phone systems with the phone lines already connected. Networks will also be in place, with any necessary routers and switches plugged in and turned on. Desks will have desktop PCs installed and waiting, and server areas will be replete with the necessary hardware to support business-critical functions. Within a few hours, a hot site can become a fully functioning element of an organization.

Hotlink – Is a method of copying information from one document (the source document) to another (the destination document) so that the destination document's information is updated automatically when the source document's information changes.

Hybrid Attack – Is a password-cracking attack that builds on the dictionary attack method by adding numerals and symbols to dictionary words.

Hybrid security control – Is a security control that is implemented in an information system in part as a common control and in part as a system-specific control. See Common Control and System-Specific Security Control.

Hyperlink - In a hypertext system, an underlined or otherwise emphasized word or phrase that displays another document when clicked with the mouse.

Hypertext - A method of preparing and publishing text, ideally suited to the computer, in which readers can choose their own paths through the material. In preparing hypertext, information is first "chunked" into small, manageable units, such as single pages of text. These units are called nodes. Then the hyperlinks (also called anchors) are embedded in the text. When a reader clicks on a hyperlink, the hypertext software displays a different node. The process of navigating among the nodes linked in this way is called browsing. A collection of nodes that are interconnected by hyperlinks is called a Web.

Hypertext Markup Language (HTML) - A set of standards used to tag the elements of a document. It is the standard protocol for formatting and displaying documents on the World Wide Web.

Hypertext Transfer Protocol (HTTP) - One of the Internet Protocol (IP) suites of protocols. Hypertext documents can be transported across a network (usually the Internet) using this protocol.

Hypertext Transfer Protocol Secure (HTTPS) - The protocol for accessing a secure Web server. Using HTTPS in the URL instead of HTTP directs the message to a secure port number rather than the default Web port number of 80. The session is then managed by a security protocol, such as Secure Sockets Layer (SSL).

I

IA architecture – Is a description of the structure and behavior for an enterprise's security processes, information security systems, personnel and organizational sub-units, showing their alignment with the enterprise's mission and strategic plans.

IA infrastructure - The underlying security framework that lies beyond an enterprise's defined boundary, but supports its IA and IA-enabled products, its security posture and its risk management plan.

IA product - Product whose primary purpose is to provide security services (e.g., confidentiality, authentication, integrity, access control, non-repudiation of data); correct known vulnerabilities; and/or provide layered defense against various categories of non-authorized or malicious penetrations of information systems or networks.

IA-enabled information technology product- Product or technology whose primary role is not security, but which provides security services as an associated feature of its intended operating capabilities. Examples include such products as security-enabled web browsers, screening routers, trusted operating systems, and security-enabled messaging systems.

IA-enabled product - Product whose primary role is not security, but provides security services as an associated feature of its intended operating capabilities.

Note: Examples include such products as security-enabled web browsers, screening routers, trusted operating systems, and security enabling messaging systems.

Identification - An act or process that presents an identifier to a system so that the system can recognize a system entity (e.g., user, process, or device) and distinguish that entity from all others.

Identifier – Is a data object - often, a printable, non-blank character string - that definitively represents a specific identity of a system entity, distinguishing that identity from all others.

Identity - The set of attribute values (i.e., characteristics) by which an entity is recognizable and that, within the scope of an identity manager's responsibility, is sufficient to distinguish that entity from any other entity.

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.

Identity token - Smart card, metal key, or other physical object used to authenticate identity.

Identity validation- Are tests enabling an information system to authenticate users or resources.

Identity-based access control - Access control based on the identity of the user (typically relayed as a characteristic of the process acting on behalf of that user) where access authorizations to specific objects are assigned based on user identity.

IMHO - A short hand appended to a comment written in an online forum, IMHO indicates that the writer is aware that they are expressing a debatable view, probably on a subject already under discussion. One of many such short hands in common use online, especially in discussion forums.

Imitative communications deception- Introduction of deceptive messages or signals into an adversary's telecommunications signals. See communications deception and manipulative communications deception.

Impact level - 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.

Implant - Electronic device or electronic equipment modification designed to gain unauthorized interception of information-bearing emanations.

Inadvertent disclosure - Type of incident involving accidental exposure of information to an individual not authorized access.

Incident - An assessed 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.

Incident response plan - The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of an incident against an organization's IT systems(s).

Incomplete Parameter Checking – Is a system flaw that exists when the operating system does not check all parameters fully for accuracy and consistency, thus making the system vulnerable to penetration.

Independent Validation Authority (IVA) - Entity that reviews the soundness of independent tests and system compliance with all stated security controls and risk mitigation actions. IVAs will be designated by the Authorizing Official as needed.

Independent Verification & Validation (IV&V) - A comprehensive review, analysis, and testing, (software and/or hardware) performed by an objective third party to confirm (i.e., verify) that the requirements are correctly defined, and to confirm (i.e., validate) that the system correctly implements the required functionality and security requirements.

Indicator - Recognized action, specific, generalized, or theoretical, that an adversary might be expected to take in preparation for an attack.

Individual accountability – The ability to associate positively the identity of a user with the time, method, and degree of access to an information system; informal security policy (C.F.D.) Natural language description, possibly supplemented by mathematical arguments, demonstrating the correspondence of the functional specification to the high-level design.

INFOCON - Information Operations Condition (INFOCON) classifications mirror Defense Conditions (DEFCON) Alert System and are a uniform system of five progressive readiness conditions– INFOCON 5 thru INFOCON 1 with INFOCON 5 being a level of normal readiness and INFOCON 1 a level of maximum readiness, implemented because of severe threat or attack. As the INFOCON levels increase,

elements of network functionality or services deemed lower priority or at high risk of attack may be temporarily suspended. Thus, CNA tools that work during a normal state of readiness may be rendered ineffective if the services or applications they exploit are turned off.

Information - Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual.

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

Information Assurance (IA) professional - Individual who works IA issues and has real world experience plus appropriate IA training and education commensurate with their level of IA responsibility.

Information Assurance Component (IAC) – Is an application (hardware and/or software) that provides one or more Information Assurance capabilities in support of the overall security and operational objectives of a system.

Information Assurance Vulnerability Alert (IAVA) - Notification that is generated when an Information Assurance vulnerability may result in an immediate and potentially severe threat to DoD systems and information; this alert requires corrective action because of the severity of the vulnerability risk.

Information domain - A three-part concept for information sharing, independent of, and across information systems and security domains that 1) identifies information sharing participants as individual members, 2) contains shared information objects, and 3) provides a security policy that identifies the roles and privileges of the members and the protections required for the information objects.

Information environment - Aggregate of individuals, organizations, and/or systems that collect, process, or disseminate information, also included is the information itself.

Information flow control – Is the procedure to ensure that information transfers within an information system are not made in violation of the security policy.

Information management – Is the planning, budgeting, manipulating, and controlling of information throughout its life cycle.

Information operations (IO) - The integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt, or usurp adversarial human and automated decision making process, information, and information systems while protecting our own.

Inf

Information owner – Is the official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, classification, collection, processing, dissemination, and disposal; See also information steward; Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.

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

Information Resources Management (IRM) - The planning, budgeting, organizing, directing, training, controlling, and management activities associated with the burden, collection, creation, use, and dissemination of information by agencies.

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

Information security policy - Aggregate of directives, regulations, rules, and practices that prescribe how an organization manages, protects, and distributes information.

Information Sharing Environment (ISE) - An approach that facilitates the sharing of terrorism and homeland security information; ISE in its broader application enables those in a trusted partnership to share, discover, and access controlled information.

Information steward – Is an agency official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.

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

> Note: Information systems also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems.

Information system life cycle - The phases which an information system passes, typically characterized as initiation, development, operation, and termination (i.e., sanitization, disposal and/or destruction).

Information Systems Security (INFOSEC)- Protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats.

Information Systems Security Engineer (ISSE) - Individual assigned responsibility for conducting information system security engineering activities; Process of capturing and refining information protection requirements to ensure their integration into information systems acquisition and information systems development through purposeful security design or configuration.

Information systems security equipment modification- Modification of any fielded hardware, firmware, software, or portion thereof, under NSA configuration control. There are three classes of modifications: mandatory (to include human safety); optional/special mission modifications; and repair actions. These classes apply to elements, subassemblies, equipment, systems, and software packages performing functions such as key generation, key distribution, message encryption, decryption, authentication, or those mechanisms necessary to satisfy security policy, labeling, identification, or accountability.

Information Systems Security Manager (ISSM) - Individual responsible for the information assurance of a program, organization, system, or enclave.

Information Systems Security Officer (ISSO) - Individual assigned responsibility for maintaining the appropriate operational security posture for an information system or program.

Information systems security product- Is an item (chip, module, assembly, or equipment), technique, or service that performs or relates to information systems security.

Information Technology (IT) - Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information 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.

Information Technology (IT) - Common term used to describe computers and automated data processing.

Information type – Is 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.

Information value - A qualitative measure of the importance of the information based upon factors such as: level of robustness of the Information Assurance controls allocated to the protection of information based upon: mission criticality, the sensitivity (e.g., classification and compartmentalization) of the information, releasability to other countries, perishability/longevity of the information (e.g., short life data versus long life intelligence source data), and potential impact of loss of confidentiality and integrity and/or availability of the information.

Information Warfare (IW) – Actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while defending one's own information, information-based processes, information systems, and computer-based networks

Initialize- Is setting the state of a cryptographic logic prior to key generation, encryption, or other operating mode.

Inside(r) threat - An entity with authorized access (i.e., within the security domain) that has the potential to harm an information system or enterprise through destruction, disclosure, modification of data, and/or denial of service.

Inspectable space- Three dimensional space surrounding equipment that processes classified and/or sensitive information within which TEMPEST exploitation is not considered practical or where legal authority to identify and remove a potential TEMPEST exploitation exists; Synonymous with: zone of control.

Integrity - The property whereby an entity has not been modified in an unauthorized manner; Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

Integrity check value - Checksum capable of detecting modification of an information system.

Intellectual property - Creations of the mind such as musical, literary, and artistic works; inventions; and symbols, names, images, and designs used in commerce, including copyrights, trademarks, patents, and related rights. Under intellectual property law, the holder of one of these abstract "properties" has certain exclusive rights to the creative work, commercial symbol, or invention by which it is covered.

Interconnection Security Agreement (ISA) – Is a document that regulates security-relevant aspects of an intended connection between an agency and an external system. It regulates the security interface between any two systems operating under two different distinct authorities. It includes a variety of descriptive, technical, procedural, and planning information. It is usually preceded by a formal MOA/MOU that defines high-level roles and responsibilities in management of a cross-domain connection.

Interface - Common boundary between independent systems or modules where interactions take place.

Int

Interface control document- Technical document describing interface controls and identifying the authorities and responsibilities for ensuring the operation of such controls. This document is base lined during the preliminary design review and is maintained throughout the information system lifecycle. Temporary authorization to test an information system in a specified operational information environment within the timeframe and under the conditions or constraints enumerated in the written authorization.

Internal network - A network where 1) the establishment, maintenance, and provisioning of security controls are under the direct control of organizational employees or contractors; or 2) cryptographic encapsulation or similar security technology implemented between organization-controlled endpoints provides the same effect (at least with regard to confidentiality and integrity). An internal network is typically organization-owned, yet may be organization-controlled while not being organization-owned.

Internal security controls - Hardware, firmware, or software features within an information system that restrict access to resources to only authorized subjects.

Internet - The Internet is the single, interconnected, worldwide system of commercial, governmental, educational, and other computer networks that share (a) the protocol suite specified by the IAB and (b) the name and address spaces managed by the Internet Corporation for Assigned Names and Numbers (ICANN).

IMAP (Internet Message Access Protocol) - IMAP is gradually replacing *POP* as the main protocol used by email *clients* in communicating with email *servers*. Using IMAP an email client program can not only retrieve email but can also manipulate message stored on the server, without having to actually retrieve the messages. So messages can be deleted, have their status changed, multiple mail boxes can be managed, etc.

Internet Protocol (IP) - Standard protocol for transmission of data from source to destinations in packet-switched communications networks and interconnected systems of such networks.

Internet Protocol (IP) - The method or protocol by which data is sent from one computer to another on the Internet.

Internet Service Provider (ISP) – Is a company that provides internet access to customers.

Intranet - A private network that is employed within the confines of a given enterprise (e.g., internal to a business or agency).

Intrusion - Unauthorized act of bypassing the security mechanisms of a system.

Intrusion Detection Systems (IDS) - Hardware or software products that gather and analyze information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organizations) and misuse (attacks from with the organizations); A security management system for computers and networks. An IDS gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks from within the organization).

Intrusion Detection System (IDS) – A computer or network monitoring system that matches observations against patterns of known or suspected unauthorized activity.

Intrusion Detection Systems (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.

Intrusion Detection Systems (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.

Intrusion Prevention System (IPS) – An inline system or software that applies IDS-style logic and approves or rejects network traffic, program and data access, hardware use, etc.

Intrusion Prevention System (IPS) - System that can detect an intrusive activity and can also attempt to stop the activity, ideally before it reaches its targets.

IP (Internet Protocol) Address - A computer's inter-network address, written as a series of four 8-bit numbers separated by periods, such as 74.125.224.72. Every website has an IP Address which corresponds to a domain name (i.e. www.google.com).

IP Number - Sometimes called a dotted quad. A unique number consisting of 4 parts separated by dots, e.g.165.113.245.2 every machine that is on the Internet has a unique IP number - if a machine does not have an IP number, it is not really on the Internet. Many machines (especially servers) also have one or more Domain Names that are easier for people to remember.

IP Security (IPSec) - Suite of protocols for securing Internet Protocol (IP) communications at the network layer, layer 3 of the OSI model by authenticating and/or encrypting each IP packet in a data stream. IPSec also includes protocols for cryptographic key establishment.

IPv4 - (Internet Protocol, version 4) the most widely used version of the Internet Protocol (the "IP" part of *TCP/IP*.) IPv4 allows for a theoretical maximum of approximately four billion *IP Numbers* (technically 2^{32}), but the actual number is far less due to inefficiencies in the way blocks of numbers are handled by networks. The gradual adoption of *IPv6* will solve this problem.

IPv6 - (Internet Protocol, version 6) the successor to *IPv4*. Already deployed in some cases and gradually spreading, IPv6 provides a huge number of available *IP Numbers* - over a sextillion addresses (theoretically 2^{128}). IPv6 allows every device on the planet to have its own IP Number.

IRC – Is basically a huge multi-user live chat facility. There are a number of major IRC *servers* around the world which are linked to each other. Anyone can create a channel and anything that anyone types in a given channel is seen by all others in the channel. Private channels can (and are) created for multi-person conference calls.

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

J

Jamming - An attack in which a device is used to emit electromagnetic energy on a wireless network's frequency to make it unusable. An attack that attempts to interfere with the reception of broadcast communications.

Java - Java is a network-friendly programming language invented by Sun Microsystems. Java is often used to build large, complex systems that involve several different computers interacting across networks, for example transaction processing systems. Java is also used to create software with graphical user interfaces such as editors, audio players, web browsers, etc. Java is also popular for creating programs that run in small electronic device/s, such as mobile telephones. Using small Java programs (called "*Applets*"), Web pages can include functions such as animations, calculators, and other fancy tricks.

JavaScript- JavaScript is a programming language that is mostly used in web pages, usually to add features that make the web page more interactive. When JavaScript is included in an *HTML* file it relies upon the browser to interpret the JavaScript. When JavaScript is combined with *Cascading Style Sheets* (CSS), and later versions of HTML (4.0 and later) the result is often called *DHTML*.

JDK - (Java Development Kit) a software development package from Sun Microsystems that implements the basic set of tools needed to write, test and debug *Java* applications and *applets*

Joint Authorization – Is a security authorization involving multiple authorizing officials.

JPEG - JPEG is most commonly mentioned as a format for image files. JPEG format is preferred to the *GIF* format for photographic images as opposed to line art or simple logo art.

K

Key – A value used to control cryptographic operations, such as decryption, encryption, signature generation, or signature verification. A numerical value used to control cryptographic operations, such as decryption, encryption, signature generation, or signature verification. A parameter used in conjunction with a cryptographic algorithm that determines its operation.
Examples applicable to this Standard include:

1. The computation of a digital signature from data, and
2. The verification of a digital signature.

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

Key Distribution Center (KDC) – COMSEC facility generating and distributing key in electronic form.

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

1. The processes of managing (e.g., generating, storing, transferring, auditing) the two components of a cryptographic key by two key component holders.
2. A key recovery technique for storing knowledge of a cryptographic key, or parts thereof, in the custody of one or more third parties called "escrow agents," so that the key can be recovered and used in specified circumstances.

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").

Key Establishment – The process by which cryptographic keys are securely established 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); The process by which cryptographic keys are securely established among cryptographic modules using key transport and/or key agreement procedures. See Key Distribution.

Key

Key Exchange – Is the process of exchanging public keys in order to establish secure communications. Process of exchanging public keys (and other information) in order to establish secure communications.

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

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

Key List – Printed series of key settings for a specific cryptonet. Key lists may be produced in list, pad, or printed tape format.

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

Key Logger – A program designed to record which keys are pressed on a computer keyboard used to obtain passwords or encryption keys and thus bypass other security measures.

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.

Key Management Device – A unit that provides for secure electronic distribution of encryption keys to authorized users.

Key Management Infrastructure – (KMI) All parts – computer hardware, firmware, software, and other equipment and its documentation; facilities that house the equipment and related functions; and companion standards, policies, procedures, and doctrine that form the system that manages and supports the ordering and delivery of cryptographic material and related information products and services to users.

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

Key Production Key (KPK) – Key used to initialize a key stream generator for the production of other electronically generated key.

Key Recovery – Mechanisms and processes that allow authorized parties to retrieve the cryptographic key used for data confidentiality.

Key Stream – Sequence of symbols (or their electrical or mechanical equivalents) produced in a machine or auto-manual cryptosystem to combine with plain text to produce cipher text, control transmission security processes, or produce key.

Key Tag – Identification information associated with certain types of electronic key.

Key Tape – Punched or magnetic tape containing key. Printed key in tape form is referred to as a key list.

Key Transport – Is the secure transport of cryptographic keys from one cryptographic module to another module.

Key Updating – Irreversible cryptographic process for modifying key.

Key Wrap – Is a method of encrypting keying material (along with associated integrity information) that provides both confidentiality and integrity protection using a symmetric key algorithm.

Key-Auto-Key (KAK) – Cryptographic logic using previous key to produce key.

Key-Encryption-Key (KEK) - Key that encrypts or decrypts other key for transmission or storage.

Keyed-hash based message authentication code (HMAC) – A message authentication code that uses a cryptographic key in conjunction with a hash function.

Keying Material – Is the key, code, or authentication information in physical, electronic, or magnetic form.

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.

KMI Operating Account (KOA) – A KMI business relationship that is established 1) to manage the set of user devices that are under the control of a specific KMI customer organization, and 2) to control the distribution of KMI products to those devices.

KMI Protected Channel (KPC) – A KMI Communication Channel that provides 1) Information Integrity Service; 2) either Data Origin Authentication Service or Peer Entity Authentication Service, as is appropriate to the mode of communications; and 3) optionally, Information Confidentiality Service.

KMI-Aware Device – A user device that has a user identity for which the registration has significance across the entire KMI (i.e., the identity's registration data is maintained in a database at the PRSN level of the system, rather than only at an MGC) and for which a product can be generated and wrapped by a PSN for distribution to the specific device.

KOA Agent – A user identity that is designated by a KOA manager to access PRSN product delivery enclaves for the purpose of retrieving wrapped products that have been ordered for user devices that are assigned to that KOA.

KOA Manager – The Management Role that is responsible for the operation of one or KOA's (i.e., manages distribution of KMI products to the end cryptographic units, fill devices, and ADPs that are assigned to the manager's KOA).

KOA Registration Manager – The individual responsible for performing activities related to registering KOAs.

L

Labeled Security Protections – Is an access control protection features of a system that use security labels to make access control decisions.

Laboratory Attack – Is the use of sophisticated signal recovery equipment in a laboratory environment to recover information from data storage media.

Leased Line - Refers to line such as a telephone line or fiber-optic cable that is rented for exclusive 24-hour, 7-days-a-week use from your location to another location. The highest speed data connections require a leased line.

Least Privilege – The security objective of granting users only those accesses they need to perform their official duties. The principle that security architecture should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function.

Least Trust – The principal that security architecture should be designed in a way that minimizes the number of components that require trust and the extent to which each component is trusted.

Level of Concern – Rating assigned to an information system indicating the extent to which protection measures, techniques, and procedures must be applied. High, Medium, and Basic are identified levels of concern. A separate Level-of-Concern is assigned to each information system for confidentiality, integrity, and availability.

Level of Protection – Extent to which protective measures, techniques, and procedures must be applied to information systems and networks based on risk, threat, vulnerability, system interconnectivity considerations, and information assurance needs. Levels of protection are: 1. Basic: information systems and networks requiring implementation of standard minimum security countermeasures. 2. Medium: information systems and networks requiring layering of additional safeguards above the standard minimum security countermeasures. 3. High: information systems and networks requiring the most stringent protection and rigorous security countermeasures.

Likelihood of Occurrence – In Information Assurance risk analysis, a weighted factor based on a subjective analysis of the probability that a given threat is capable of exploiting a given vulnerability.

Limited Maintenance – COMSEC maintenance restricted to fault isolation, removal, and replacement of plug-in assemblies. Soldering or unsoldering usually is prohibited in limited maintenance. See Full Maintenance.

Line Conditioning – Elimination of unintentional signals or noise induced or conducted on a telecommunications or information system signal, power, control, indicator, or other external interface line.

Line Conduction – Unintentional signals or noise induced or conducted on a telecommunications or information system signal, power, control, indicator, or other external interface line.

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; Encryption of information between nodes of a communications system.

List-Oriented – Information system protection in which each protected object has a list of all subjects authorized to access it.

Local Access – Access to an organizational information system by a user (or process acting on behalf of a user) communicating through a direct connection without the use of a network.

Local Area Network (LAN) - A group of computers and associated devices that share a common communications line or wireless link. Typically, connected devices share the resources of a single processor or server within a small geographic area (for example, within an office building). Usually, the server has applications and data storage that are shared in common by multiple computer users; a computer network limited to the immediate area, usually the same building or floor of a building.

Local Authority – Organization responsible for generating and signing user certificates in a PKI-enabled environment.

Local Management Device/Key Processor (LMD/KP) – EKMS platform providing automated management of COMSEC material and generating key for designated users.

Logic Bomb – A piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met.

Logic Bomb -A piece of programming code intentionally inserted into a software system that will cause a malicious function to occur when one or more specified conditions are met.

Logical Completeness Measure – Means for assessing the effectiveness and degree to which a set of security and access control mechanisms meets security specifications.

Logical Perimeter – A conceptual perimeter that extends to all intended users of the system, both directly and indirectly connected, who receive output from the system without a reliable human review by an appropriate authority. The location of such a review is commonly referred to as an "air gap."

Low Impact – The loss of confidentiality, integrity, or availability that could be expected to have a limited adverse effect on organizational operations, organizational assets, individuals, other organizations, or the national security interests of the United States; (i.e., 1) causes a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; 2) results in minor damage to organizational assets; 3) results in minor financial loss; or 4) results in minor harm to individuals).

Low Probability of Detection – Result of measures used to hide or disguise intentional electromagnetic transmissions.

Low Probability of Intercept – Result of measures to prevent the intercept of intentional electromagnetic transmissions. The objective is to minimize an adversary's capability of receiving, processing, or replaying an electronic signal.

Low-Impact System - An information system in which all three security objectives (i.e., confidentiality, integrity, and availability) are assigned a FIPS 199 potential impact value of low; An information system in which all three security properties (i.e., confidentiality, integrity, and availability) are assigned a potential impact value of low.

LulzSec –Is a splinter "hacktivist" group that branched off from Anonymous in May 2011 and shares similar social and political motivations. The two groups appear to have similar agendas and overlapping membership.

M

Macro Virus – Is a virus that attaches itself to documents and uses the macro programming capabilities of the document's application to execute and propagate.

Magnetic Remanence – Magnetic representation of residual information remaining on a magnetic medium after the medium has been cleared. See Clearing.

Maintenance Hook – Special instructions (trapdoors) in software allowing easy maintenance and additional feature development. Since maintenance hooks frequently allow entry into the code without the usual checks, they are a serious security risk if they are not removed prior to live implementation.

Maintenance Key – Key intended only for in-shop use.

Major Application – Is 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.

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.

Malicious Applets – Are small application programs that are automatically downloaded and executed and that perform an unauthorized function on an information system.

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. Spyware and some forms of adware are also examples of malicious code.

Malicious Logic – Hardware, firmware, or software that is intentionally included or inserted in a system for a harmful purpose.

Malware – Is 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; a virus, worm, Trojan horse, or other code-based malicious entity that successfully infects a host; a generic term for a number of different types of malicious code.

Management Client (MGC) – A configuration of a client node that enables a KMI external operational manager to manage KMI products and services by either 1) accessing a PRSN, or 2) exercising locally provided capabilities. An MGC consists of a client platform and an advanced key processor (AKP).

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. Actions taken to manage the development, maintenance, and use of the system, including system-specific policies, procedures and rules of behavior, individual roles and responsibilities, individual accountability, and personnel security decisions.

Management Security 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 systems security.

Mandatory Access Control (MAC) – 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.

Mandatory Access Control – 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; A means of restricting access to objects based on the sensitivity (as represented by a security label) of the information contained in the objects and the formal authorization (i.e., clearance, formal access approvals, and need-to-know) of subjects to access information of such sensitivity.

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; A form of active wiretapping attack in which the attacker intercepts and selectively modifies communicated data to masquerade as one or more of the entities involved in a communication association.

Man-in-the-Middle Attack - Posing as an online bank or merchant, a cyber criminal allows a victim to sign in over a Secure Sockets Layer (SSL) connection. The attacker then logs onto the real server using the client's information and steals credit card numbers. See also SSL and Server.

Manipulative Communications Deception – Alteration or simulation of friendly telecommunications for the purpose of deception. See Communications Deception and Imitative Communications Deception.

Manual Cryptosystem – Cryptosystem in which the cryptographic processes are performed without the use of crypto-equipment or auto-manual devices.

Manual Key Transport – Is a non-automated means of transporting cryptographic keys by physically moving a device, document, or person containing or possessing the key or key component; a nonelectric means of transporting cryptographic keys.

Manual Remote Rekeying – Procedure by which a distant crypto-equipment is rekeyed electronically, with specific actions required by the receiving terminal operator. Synonymous with: cooperative remote rekeying. See also Automatic Remote Keying.

Masquerading – When an unauthorized agent claims the identity of another agent, it is said to be masquerading; A type of threat action whereby an unauthorized entity gains access to a system or performs a malicious act by illegitimately posing as an authorized entity.

Master Cryptographic Ignition Key – Is key device with electronic logic and circuits providing the capability for adding more operational CIKs to a keyset.

Match/matching – The process of comparing biometric information against a previously stored template(s) and scoring the level of similarity.

Maximum Tolerable Downtime – The amount of time mission/business processes can be disrupted without causing significant harm to the organization's mission.

Mechanism – An assessment object that includes specific protection-related items (e.g., hardware, software, or firmware) employed within or at the boundary of an information system.

Media – Physical devices or writing surfaces including but not limited to magnetic tapes, optical disks, magnetic disks, Large Scale Integration (LSI) memory chips, and printouts (but not including display media) onto which information is recorded, stored, or printed within an information system.

Media Sanitization – Is a general term referring to the actions taken to render data written on media unrecoverable by both ordinary and extraordinary means; the actions taken to render data written on media unrecoverable by both ordinary and extraordinary means.

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; A document established between two or more parties to define their respective responsibilities in accomplishing a particular goal or mission, e.g., establishing, operating, and securing a system interconnection.

Memory Scavenging – Is the collection of residual information from data storage.

Message Authentication Code – (MAC) a cryptographic checksum on data that uses a symmetric key to detect both accidental and intentional modifications of the data. MACs provide authenticity and integrity protection, but not non-repudiation protection; A cryptographic checksum that results from passing data through a message authentication algorithm.

Message Digest – The result of applying a hash function to a message. Also known as a "hash value" or "hash output"; A digital signature that uniquely identifies data and has the property that changing a single bit in the data will cause a completely different message digest to be generated. A cryptographic checksum typically generated for a file that can be used to detect changes to the file.

Message Externals – Information outside of the message text, such as the header, trailer, etc.

Message Indicator – Sequence of bits transmitted over a communications system for synchronizing cryptographic equipment.

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

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

Minimalist Cryptography – Cryptography that can be implemented on devices with very limited memory and computing capabilities, such as RFID tags.

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.

Mirror - Generally speaking, "to mirror" is to maintain an exact copy of something. Probably the most common use of the term on the Internet refers to "mirror sites" which are *web* sites, or *FTP* sites that maintain copies of material originated at another location, usually in order to provide more widespread access to the resource. For example, one site might create a library of software, and 5 other sites might maintain mirrors of that library.

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.

Mission Assurance Category – (MAC) A Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) term primarily used to determine the requirements for availability and integrity.

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.

Mission/Business Segment – Elements of organizations describing mission areas, common/shared business services, and organization-wide services. Mission/business segments can be identified with one or more information systems which collectively support a mission/business process.

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; A program (e.g., script, macro, or other portable instruction) that can be shipped unchanged to a heterogeneous collection of platforms and executed with identical semantics. 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.

> Note: Some examples of software technologies that provide the mechanisms for the production and use of mobile code include Java, JavaScript, ActiveX, VBScript, etc.

Mobile Code Technologies – Are software technologies that provide the mechanisms for the production and use of mobile code (e.g., Java, JavaScript, ActiveX, and VBScript).

Mo

Mobile Device – Portable cartridge/disk-based, removable storage media (e.g., floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory; Portable computing and communications device with information storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices).

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.

Mode of Operation – An algorithm for the cryptographic transformation of data that features a symmetric key block cipher algorithm; Description of the conditions under which an information system operates based on the sensitivity of information processed and the clearance levels, formal access approvals, and need-to-know of its users. Four modes of operation are authorized for processing or transmitting information: dedicated mode, system high mode, compartmented/partitioned mode, and multilevel mode.
SOURCE: CNSSI-4009

Modem - (MOdulator, DEModulator)- A device that connects a computer to a phone line; a telephone for a computer. A modem allows a computer to talk to other computers through the phone system. Basically, modems do for computers what a telephone does for humans. The maximum practical *bandwidth* using a modem over regular telephone lines is currently around 57,000 *bps*.

Modem - A device that modulates outgoing digital signals from a computer or other digital device to analog signals for a conventional copper twisted pair telephone line, then demodulates the incoming analog signal and converts it back to digital signals.

Moderate Impact – The loss of confidentiality, integrity, or availability that could be expected to have a serious adverse effect on organizational operations, organizational assets, individuals, other organizations, or the national security interests of the United States; (i.e., 1) causes a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; 2) results in significant damage to organizational assets; 3) results in significant financial loss; or 4) results in significant harm to individuals that does not involve loss of life or serious life threatening injuries).

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; An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a potential impact value of moderate and no security objective is assigned a potential impact value of high.

Mousetrapping - A technique that prevents a user from "escaping" from an objectionable Web site. The result can be a never-ending stream of pop up Web sites, which clutter the screen and often cause panic and distress to the user.

Multifactor Authentication – Authentication using two or more factors to achieve authentication. Factors include: (i) something you know (e.g. password/PIN); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric). See Authenticator.

Multi-Hop Problem - The security risks resulting from a mobile software agent visiting several platforms.

Multilevel Device – Equipment trusted to properly maintain and separate data of different security domains.

Multilevel Mode – Mode of operation wherein all the following statements are satisfied concerning the users who have direct or indirect access to the system, its peripherals, remote terminals, or remote hosts: 1) some users do not have a valid security clearance for all the information processed in the information system; 2) all users have the proper security clearance and appropriate formal access approval for that information to which they have access; and 3) all users have a valid need-to-know only for information to which they have access.

Multilevel Security (MLS) – Concept of processing information with different classifications and categories that simultaneously permits access by users with different security clearances and denies access to users who lack authorization.

Multiple Security Levels (MSL) – Capability of an information system that is trusted to contain, and maintain separation between, resources (particularly stored data) of different security domains.

Multi-Releasable – A characteristic of an information domain where access control mechanisms enforce policy-based release of information to authorized users within the information domain.

Mutual Authentication – This occurs when parties at both ends of a communication activity authenticate each other; the process of both entities involved in a transaction verifying each other.

Mutual Suspicion – Condition in which two information systems need to rely upon each other to perform a service, yet neither trusts the other to properly protect shared data

N

Naming Authority – Is an organizational entity responsible for assigning distinguished names (DNs) and for assuring that each DN is meaningful and unique within its domain.

National Information Infrastructure – Nationwide interconnection of communications networks, computers, databases, and consumer electronics that make vast amounts of information available to users. It includes both public and private networks, the Internet, the public switched network, and cable, wireless, and satellite communications.

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

> Subparagraph (B): Does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

Need-To-Know Determination – Decision made by an authorized holder of official information that a prospective recipient requires access to specific official information to carry out official duties.

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.

Need-To-Know – A method of isolating information resources based on a user's need to have access to that resource in order to perform their job but no more. The terms 'need-to know" and "least privilege" express the same idea. Need-to-know is generally applied to people, while least privilege is generally applied to processes.

Net-centric Architecture – A complex system of systems composed of subsystems and services that are part of a continuously evolving, complex community of people, devices, information and services interconnected by a network that enhances information sharing and collaboration. Subsystems and services may or may not be developed or owned by the same entity, and, in general, will not be continually present during the full life cycle of the system of systems. Examples of this architecture include service-oriented architectures and cloud computing architectures.

Netiquette - The etiquette on the *Internet*.

Netizen - Derived from the term citizen, referring to a citizen of the *Internet*, or someone who uses networked resources. The term connotes civic responsibility and participation.

Netscape - A *WWW Browser* and the name of a company. The Netscape (tm) browser was originally based on the *Mosaic* program developed at the National Center for Supercomputing Applications (NCSA).

Network – Information system(s) implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.

Network - Two or more computer systems that are grouped together to share information, software and hardware.

Network Access – Access to an organizational information system by a user (or a process acting on behalf of a user) communicating through a network (e.g., local area network, wide area network, Internet).

Network Access Control (NAC) – A feature provided by some firewalls that allows access based on a user's credentials and the results of health checks performed on the telework client device.

Network Access Point (NAP) - Points at which Internet Service Providers (ISPs) connect with other ISP networks, allowing internet traffic to flow between the two ISP networks. See also Internet Service Provider (ISP).

Network Address Translation (NAT) – A routing technology used by many firewalls to hide internal system addresses from an external network through use of an addressing schema.

Network Behavioral Analysis (NBA) – Is an intrusion detection system that models network traffic and alerts on violations of known acceptable activity. Rules can include data volume, time of day, traffic rate, communication partners, content, and other elements.

Network Front-End – Device implementing protocols that allow attachment of a computer system to a network.

Net-No

Network Resilience – Is a computing infrastructure that provides continuous business operation (i.e., highly resistant to disruption and able to operate in a degraded mode if damaged), rapid recovery if failure does occur, and the ability to scale to meet rapid or unpredictable demands.

Network Sniffing – A passive technique that monitors network communication, decodes protocols, and examines headers and payloads for information of interest. It is both a review technique and a target identification and analysis technique.

Network Sponsor – Is an individual or organization responsible for stating the security policy enforced by the network, designing the network security architecture to properly enforce that policy, and ensuring that the network is implemented in such a way that the policy is enforced.

Network System – System implemented with a collection of interconnected components. A network system is based on a coherent security architecture and design.

Network Weaving – Penetration technique in which different communication networks are linked to access an information system to avoid detection and trace-back.

NIC (Network Information Center) - Generally, any office that handles information for a network. The most famous of these on the Internet was the InterNIC, which was where most new domain names were registered until that process was decentralized to a number of private companies. Also means "Network Interface card", which is the card in a computer that you plug a network cable into.

NIPRNET – Non-classified Internet Protocol Router Network; The unclassified network of the US Department of Defense which provides Internet access as well as interconnectivity to DoD users and facilities.

NNTP (**Network News Transport Protocol)** - The protocol used by *client* and *server* software to carry *USENET* postings back and forth over a *TCP/IP network*. If you are using any of the more common software such as *Netscape*, Nuntius, Internet Explorer, etc. to participate in *newsgroups* then you are benefiting from an NNTP connection.

Node - Any single computer connected to a *network*.

No-Lone Zone (NLZ) – Area, room, or space that, when staffed, must be occupied by two or more appropriately cleared individuals who remain within sight of each other. See Two-Person Integrity.

Nonce – A value used in security protocols that is never repeated with the same key. For example, nonce used as challenges in challenge-response authentication protocols generally must not be repeated until authentication keys are changed. Otherwise, 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; a random or non-repeating value that is included in data exchanged by a protocol, usually for the purpose of guaranteeing the transmittal of live data rather than replayed data, thus detecting and protecting against replay attacks.

Non-deterministic Random Bit Generator (NRBG) – An RBG that (when working properly) produces outputs that have full entropy. Contrast with a DRBG. Other names for non-deterministic RBGs are True Random Number (or Bit) Generators and, simply, Random Number (or Bit) Generators.

Non-Local Maintenance – Are maintenance activities conducted by individuals communicating through a network; either an external network (e.g., the Internet) or an internal network.

Non-Organizational User – Is a user who is not an organizational user (including public users).

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; Protection against an individual falsely denying having performed a particular action. Provides the capability to determine whether a given individual took a particular action such as creating information, sending a message, approving information, and receiving a message; 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); A service that is used to provide assurance of the integrity and origin of data in such a way that the integrity and origin can be verified and validated by a third party as having originated from a specific entity in possession of the private key (i.e., the signatory).

NSA-Approved Cryptography – Cryptography that consists of: (i) an approved algorithm; (ii) an implementation that has been approved for the protection of classified information in a particular environment; and (iii) a supporting key management infrastructure.

NTLM - A Microsoft authentication protocol that uses cryptographic hash representations of account passwords.

Null – Dummy letter, letter symbol, or code group inserted into an encrypted message to delay or prevent its decryption or to complete encrypted groups for transmission or transmission security purposes.

O

Object – A passive entity that contains or receives information; Passive information system-related entity (e.g., devices, files, records, tables, processes, programs, domains) containing or receiving information. Access to an object implies access to the information it contains.

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.

Object Reuse – Reassignment and reuse of a storage medium containing one or more objects after ensuring no residual data remains on the storage medium.

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.

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.

Off-line Cryptosystem – Cryptographic system in which encryption and decryption are performed independently of the transmission and reception functions.

On-Card – Refers to data that is stored within the PIV card or computation that is done by the ICC of the PIV card.

One-part Code - Code in which plain text elements and their accompanying code groups are arranged in alphabetical, numerical, or other systematic order, so one listing serves for both encoding and decoding. One-part codes are normally small codes used to pass small volumes of low-sensitivity information.

One-time Cryptosystem – Cryptosystem employing key used only once.

One-time Pad – Manual one-time cryptosystem produced in pad form.

One-time Tape – Punched paper tape used to provide key streams on a one-time basis in certain machine cryptosystems.

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).

Online Attack – Is 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.

Online Certificate Status Protocol (OCSP) – An online protocol used to determine the status of a public key certificate.

Online Cryptosystem – Is a cryptographic system in which encryption and decryption are performed in association with the transmitting and receiving functions.

Online Service Provider (OSP) – Is a company that provides Internet access and other services such as shopping, news, chat rooms, and special events. AOL and MSN are OSPs.

Open Checklist Interactive Language (OCIL) – SCAP language for expressing security checks that cannot be evaluated without some human interaction or feedback.

Open Content - Copyrighted information (such as this Glossary) that is made available by the copyright owner to the general public under license terms that allow reuse of the material, often with the requirement (as with this Glossary) that the re-user grant the public the same rights to the modified version that the re-user received from the copyright owner. Information that is in the Public Domain might also be considered a form of Open Content.

Open Source Software - Open Source Software is software for which the underlying programming code is available to the users so that they may read it, make changes to it, and build new versions of the software incorporating their changes. There are many types of Open Source Software, mainly differing in the licensing term under which (altered) copies of the source code may (or must be) redistributed.

Open Source Software - Software for which the underlying programming code is available to the users so that they may read it, make changes to it, and build new versions of the software incorporating their changes.

Open Storage – Any storage of classified national security information outside of approved containers. This includes classified information that is resident on information systems media and outside of an approved storage container, regardless of whether or not that media is in use (i.e., unattended operations).

Open Vulnerability and Assessment Language (OVAL) – SCAP language for specifying low-level testing procedures used by checklists.

Operating System (OS) Programs that manage all the basic functions and programs on a computer, such as allocating system resources, providing access and security controls, maintaining file systems and managing communications between end users and hardware devices. Examples include Microsoft's Windows, Apple's Macintosh and Red Hat's Linux.

Operating System (OS) Fingerprinting – Is analyzing characteristics of packets sent by a target, such as packet headers or listening ports, to identify the operating system in use on the target.

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). The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by people (as opposed to systems).

Operational Key – Key intended for use over-the-air for protection of operational information or for the production or secure electrical transmission of key streams.

Operational Vulnerability Information – Information that describes the presence of information vulnerability within a specific operational setting or network.

Operational Waiver – Authority for continued use of unmodified COMSEC end-items pending the completion of a mandatory modification.

Operations Code – Code composed largely of words and phrases suitable for general communications use.

Operations Security (OPSEC) – Systematic and proven process by which potential adversaries can be denied information about capabilities and intentions by identifying, controlling, and protecting generally unclassified evidence of the planning and execution of sensitive activities. The process involves five steps: identification of critical information, analysis of threats, analysis of vulnerabilities, assessment of risks, and application of appropriate countermeasures.

Optional Modification – NSA-approved modification not required for universal implementation by all holders of a COMSEC end-item. This class of modification requires all of the engineering/doctrinal control of mandatory modification but is usually not related to security, safety, TEMPEST, or reliability.

Organization – A federal agency, or, as appropriate, any of its operational elements. An entity of any size, complexity, or positioning within an organizational structure (e.g., a federal agency, or, as appropriate, any of its operational elements).

Organizational Information Security Continuous Monitoring – Ongoing monitoring sufficient to ensure and assure effectiveness of security controls related to systems, networks, and cyberspace, by assessing security control implementation and organizational security status in accordance with organizational risk tolerance – and within a reporting structure designed to make real-time, data-driven risk management decisions.

Organizational Maintenance – Limited maintenance performed by a user organization.

Organizational Registration Authority (ORA) – Entity within the PKI that authenticates the identity and the organizational affiliation of the users.

Organizational User – An organizational employee or an individual the organization deems to have equivalent status of an employee (e.g., contractor, guest researcher, individual detailed from another organization, individual from allied nation).

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.

Outside(r) Threat – Is an unauthorized entity outside the security domain that has the potential to harm an information system through destruction, disclosure, modification of data, and/or denial of service.

Overt Channel – Communications path within a computer system or network designed for the authorized transfer of data.

Overt Testing – Security testing performed with the knowledge and consent of the organization's IT staff.

Over-The-Air Key Distribution – Providing electronic key via over-the-air rekeying, over-the-air key transfer, or cooperative key generation.

Over-The-Air Key Transfer – Electronically distributing key without changing traffic encryption key used on the secured communications path over which the transfer is accomplished.

Over-The-Air Rekeying (OTAR) – Changing traffic encryption key or transmission security key in remote cryptographic equipment by sending new key directly to the remote cryptographic equipment over the communications path it secures.

Overwrite Procedure – A software process that replaces data previously stored on storage media with a predetermined set of meaningless data or random patterns.

P

Packet - A piece of a message transmitted over a packet-switching network. One of the key features of a packet is that it contains the Internet Protocol addressing information in addition to the data.

Packet Filter – Is a routing device that provides access control functionality for host addresses and communication sessions.

Packet Sniffer – Software that observes and records network traffic.

Packet Switching - The method used to move data around on the *Internet*. In packet switching, all the data coming out of a machine is broken up into chunks, each chunk has the address of where it came from and where it is going. This enables chunks of data from many different sources to co-mingle on the same lines, and be sorted and directed along different routes by special machines along the way; this way many people can use the same lines at the same time. You might think of several caravans of trucks all using the same road system to carry materials.

Parity – Bit(s) used to determine whether a block of data has been altered.

Partitioned Security Mode – Information systems security mode of operation wherein all personnel have the clearance, but not necessarily formal access approval and need-to-know, for all information handled by an information system.

Passive Attack – Is 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); an attack that does not alter systems or data.

Passive Security Testing – Security testing that does not involve any direct interaction with the targets, such as sending packets to a target.

Passive Wiretapping – Is the monitoring or recording of data while it is being transmitted over a communications link, without altering or affecting the data. The monitoring or recording of unencrypted data, such as passwords transmitted in clear text, while they are being transmitted over a communications link.

Password – A secret that a Claimant memorizes and uses to authenticate his or her identity. Passwords are typically character strings; A protected character string used to authenticate the identity of a computer system user or to authorize access to system resources; A string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization; A protected/private string of letters, numbers, and/or special characters used to authenticate an identity or to authorize access to data.

Password Cracking – The process of recovering secret passwords stored in a computer system or transmitted over a network.

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; the ability to protect the contents of a file or device from being accessed until the correct password is entered.

Patch – An update to an operating system, application, or other software issued specifically to correct particular problems with the software.

Patch - An update released by a software manufacturer to fix bugs in existing programs.

Patch Management – The systematic notification, identification, deployment, installation, and verification of operating system and application software code revisions. These revisions are known as patches, hot fixes, and service packs.

Path Histories – Maintaining an authenticable 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.

Payload – The input data to the CCM generation-encryption process that is both authenticated and encrypted.

PDF (Portable Document Format)- A file format designed to enable printing and viewing of documents with all their formatting (typefaces, images, layout, etc.) appearing the same regardless of what operating system is used, so a PDF document should look the same on Windows, Macintosh, Linux, OS/2, etc. The PDF format is based on the widely used Postscript document-description language. Both PDF and Postscript were developed by the Adobe Corporation; File format and filename extension for Adobe Portable Document Format documents.

Peer Entity Authentication – The process of verifying that a peer entity in an association is as claimed.

Penetration Testing – A test methodology in which assessors, using all available documentation (e.g., system design, source code, manuals) and working under specific constraints, attempt to circumvent the security features of an information system; A test methodology in which assessors, typically working under specific constraints, attempt to circumvent or defeat the security features of an information system; Security testing in which evaluators mimic real-world attacks in an attempt to identify ways to circumvent the security features of an application, system, or network. Penetration testing often involves issuing real attacks on real systems and data, using the same tools and techniques used by actual attackers. Most penetration tests involve looking for combinations of vulnerabilities on a single system or multiple systems that can be used to gain more access than could be achieved through a single vulnerability.

Per-Call Key – Unique traffic encryption key generated automatically by certain secure telecommunications systems to secure single voice or data transmissions. See Cooperative Key Generation.

Performance Reference Model – (PRM) Framework for performance measurement providing common output measurements throughout the federal government. It allows agencies to better manage the business of government at a strategic level by providing a means for using an agency's EA to measure the success of information systems investments and their impact on strategic outcomes.

Perimeter – (C&A) encompasses all those components of the system that are to be accredited by the DAA, and excludes separately accredited systems to which the system is connected. (Authorization) Encompasses all those components of the system or network for which a Body of Evidence is provided in support of a formal approval to operate.

Periods Processing – The processing of various levels of classified and unclassified information at distinctly different times. Under the concept of periods processing, the system must be purged of all information from one processing period before transitioning to the next.

Perishable Data – Information whose value can decrease substantially during a specified time. A significant decrease in value occurs when the operational circumstances change to the extent that the information is no longer useful.

Permalink – Is a "permanent link" to a particular posting in a *blog*. A permalink is a *URL* that points to a specific blog posting, rather than to the page in which the posting original occurred (which may no longer contain the posting.)

Permuter – Device used in cryptographic equipment to change the order in which the contents of a shift register are used in various nonlinear combining circuits.

Personal Firewall – A utility on a computer that monitors network activity and blocks communications that are unauthorized.

Personal Identification Number – (PIN) A password consisting only of decimal digits; a secret that a claimant memorizes and uses to authenticate his or her identity. PINs are generally only decimal digits; an alphanumeric code or password used to authenticate an identity.

Personal Identity Verification – (PIV) The process of creating and using a government wide secure and reliable form of identification for federal employees and contractors, in support of HSPD 12, Policy for a Common Identification Standard for Federal Employees and Contractors.

Personal Identity Verification Accreditation – The official management decision to authorize operation of a PIV Card Issuer after determining that the Issuer's reliability has satisfactorily been established through appropriate assessment and certification processes.

Personal Identity Verification Authorizing Official – Is an individual who can act on behalf of an agency to authorize the issuance of a credential to an applicant.

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).

Personal Identity Verification Issuer – 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 cards with the identity credentials of the authorized subjects, and delivers the personalized card to the authorized subjects along with appropriate instructions for protection and use.

Personal Identity Verification Registrar – Is an entity that establishes and vouches for the identity of an applicant to a PIV Issuer. The PIV RA authenticates the applicant's identity by checking identity source documents and identity proofing, and that ensures a proper background check has been completed, before the credential is issued.

Personal Identity Verification Sponsor- Is an individual who can act on behalf of a department or agency to request a PIV Card for an applicant.

Pers-PI

Personally Identifiable Information – (PII) Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.; Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

Personnel Registration Manager – The management role that is responsible for registering human users, i.e., users that are people.

Pharming - Redirecting visitors from a real website to a bogus one. A user enters what is believed to be a valid Web address and is unknowingly redirected to an illegitimate site that steals the user's personal information. On the spoofed site, criminals may mimic real transactions and harvest private information unknowingly shared by users. With this, the attacker can then access the real website and conduct transactions using the credentials of a valid user.

Phishing – Tricking individuals into disclosing sensitive personal information through deceptive computer-based means; Deceiving individuals into disclosing sensitive personal information through deceptive computer-based means; A digital form of social engineering that uses authentic-looking—but bogus—emails to request information from users or direct them to a fake Web site that requests information.

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

Phishing – The practice of enticing a victim to visit a website or other online resource with the intention of stealing credentials, financial information such as bank accounts, or credit card numbers. Phishing attacks generally involve an email claiming to come from a trusted entity such as a bank or ecommerce vendor, with a link to a website and the instructions to click the link and take actions once at the website.

Physically Isolated Network – Is a network that is not connected to entities or systems outside a physically controlled space.

Piconet – A small Bluetooth network created on an ad hoc basis that includes two or more devices.

PII Confidentiality Impact Level – The PII confidentiality impact level—low, moderate, or high—indicates the potential harm that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed.

Ping - To check if a server is running; from the sound that a sonar system makes in movies, you know when they are searching for a submarine.

Plaintext – Data input to the Cipher or output from the Inverse Cipher; Intelligible data that has meaning and can be understood without the application of decryption.

Plaintext Key – Is an unencrypted cryptographic key.

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.

Plug-in - A (usually small) piece of software that adds features to a larger piece of software. Common examples are plug-ins for the Netscape® *browser* and web*server*. Adobe Photoshop® also uses plug-ins.

Point of Presence (POP) - The point through which local internet users connect to their Internet Service Provider's (ISP) network, often through a modem or dedicated line

Two commonly used meanings:

- Point of Presence and Post Office Protocol.
  - A Point of Presence usually means a city or location where a network can be connected to, often with dial up phone lines. So if an Internet company says they will soon have a POP in Belgrade, it means that they will soon have a local phone number in Belgrade and/or a place where leased lines can connect to their network.
- A second meaning, Post Office Protocol refers to a way that e-mail *client* software such as Eudora gets mail from a mail *server*. When you obtain an account from an Internet Service Provider (*ISP*) you almost always get a POP account with it, and it is this POP account that you tell your e-mail software to use to get your mail. Another protocol called IMAP is replacing POP for email.

Point to Point Protocol (PPP)- The most common protocol used to connect home computers to the Internet over regular phone lines.
Most well known as a protocol that allows a computer to use a regular telephone line and a *modem* to make *TCP/IP* connections and thus be really and truly on the *Internet*.

Policy Approving Authority (PAA) – Is a first level of the PKI Certification Management Authority that approves the security policy of each PCA.

Policy Certification Authority (PCA) – Is a second level of the PKI Certification Management Authority that formulates the security policy under which it and its subordinate CAs will issue public key certificates.

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.

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.

Policy-Based Access Control (PBAC) - A form of access control that uses an authorization policy that is flexible in the types of evaluated parameters (e.g., identity, role, clearance, operational need, risk, and heuristics).

Pop-up - A browser window that opens in addition to the main window. Frequently contain bothersome advertising and may be difficult to get rid of. Pop-ups may open automatically without input from the user and closing one may open several more unwanted windows.

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).

Port - A port is nothing more than an integer that uniquely identifies the endpoint of a communication stream. Only one process per machine can listen on the same port number.

Portable Network Graphics (**PNG**) - PNG is a graphics format specifically designed for use on the World Wide Web. PNG enable compression of images without any loss of quality, including high-resolution images. Another important feature of PNG is that anyone may create software that works with PNG images without paying any fees - the PNG standard is free of any licensing costs.

Port Scanning – Using a program to remotely determine which ports on a system are open (e.g., whether systems allow connections through those ports).

Port Scanning - A port scan is a series of messages sent by someone attempting to break into a computer to learn which computer network services, each associated with a "well-known" port number, the computer provides. Port scanning gives the assailant an idea where to probe for weaknesses. Essentially, a port scan consists of sending a message to each port, one at a time. The kind of response received indicates whether the port is used and can therefore be probed for weakness. Portal a Web site or service offering a broad array of resources and services, such as e mail, search engines, subject directories, and forums.

Portable Electronic Device (PED) – Any non-stationary electronic apparatus with singular or multiple capabilities of recording, storing, and/or transmitting data, voice, video, or photo images. This includes but is not limited to laptops, personal digital assistants, pocket personal computers, palmtops, MP3 players, cellular telephones, thumb drives, video cameras, and pagers.

Portal – A high-level remote access architecture that is based on a server that offers teleworkers access to one or more applications through a single centralized interface.

Positive Control Material – Generic term referring to a sealed authenticator system, permissive action link, coded switch system, positive enable system, or nuclear command and control documents, material, or devices.

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.

Potential Impact – 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. The loss of confidentiality, integrity, or availability that could be expected to have a limited (low) adverse effect, a serious (moderate) adverse effect, or a severe or catastrophic (high) adverse effect on organizational operations, organizational assets, or individuals.

Practice Statement – A formal statement of the practices followed by an authentication entity (e.g., RA, CSP, or Verifier). It usually describes the policies and practices of the parties and can become legally binding.

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

Prediction Resistance – Prediction resistance is provided relative to time T if there is assurance that an adversary who has knowledge of the internal state of the DRBG at some time prior to T would be unable to distinguish between observations of ideal random bit strings and bit strings output by the DRBG at or subsequent to time T. The complementary assurance is called Backtracking Resistance.

Predisposing Condition – A condition that exists within an organization, a mission/business process, enterprise architecture, or information system including its environment of operation, which contributes to (i.e., increases or decreases) the likelihood that one or more threat events, once initiated, will result in undesirable consequences or adverse impact to organizational operations and assets, individuals, other organizations, or the Nation.

Preproduction Model – Version of INFOSEC equipment employing standard parts and suitable for complete evaluation of form, design, and performance. Preproduction models are often referred to as beta models.

Primary Services Node (PRSN) – Is a Key Management Infrastructure core node that provides the users' central point of access to KMI products, services, and information.

Principal – An entity whose identity can be authenticated.

Principal Accrediting Authority – (PAA) senior official with authority and responsibility for all intelligence systems within an agency.

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.

Print Suppression – Eliminating the display of characters in order to preserve their secrecy.

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

Privacy Impact Assessment (PIA) – 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.

Privacy System – Commercial encryption system that affords telecommunications limited protection to deter a casual listener, but cannot withstand a technically competent cryptanalytic attack.

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

Private Key – 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, for example, to:

1. Compute the corresponding public key,
2. Compute a digital signature that may be verified by the corresponding public key,
3. Decrypt keys that were encrypted by the corresponding public key, or
4. Compute a shared secret during a key-agreement transaction.

Private Key –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; 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 cryptography scheme, the private or secret key of a key pair which must be kept confidential and is used to decrypt messages encrypted with the public key or to digitally sign messages, which can then be validated with the public key.

Privilege – A right granted to an individual, a program, or a process.

Privilege Management – The definition and management of policies and processes that define the ways in which the user is provided access rights to enterprise systems. It governs the management of the data that constitutes the user's privileges and other attributes, including the storage, organization and access to information in directories.

Privileged Account – Is an information system account with approved authorizations of a privileged user; an information system account with authorizations of a privileged user; Individuals who have access to set "access rights" for users on a given system; sometimes referred to as system or network administrative accounts.

Privileged Command – A human-initiated command executed on an information system involving the control, monitoring, or administration of the system including security functions and associated security-relevant information.

Privileged Process – A computer process that is authorized (and, therefore, trusted) to perform security-relevant functions that ordinary processes are not authorized to perform.

Privileged User – A user that is authorized (and, therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.

Probe – A technique that attempts to access a system to learn something about the system.

Product Source Node (PSN) – Is the Key Management Infrastructure core node that provides central generation of cryptographic key material.

Production Model – Is an INFOSEC equipment in its final mechanical and electrical form.

Profiling – Measuring the characteristics of expected activity so that changes to it can be more easily identified.

Promiscuous Mode – Is a configuration setting for a network interface card that causes it to accept all incoming packets that it sees, regardless of their intended destinations.

Proprietary Information (PROPIN) – Material and information relating to or associated with a company's products, business, or activities, including but not limited to financial information; data or statements; trade secrets; product research and development; existing and future product designs and performance specifications; marketing plans or techniques; schematics; client lists; computer programs; processes; and know-how that has been clearly identified and properly marked by the company as proprietary information, trade secrets, or company confidential information. The information must have been developed by the company and not be available to the government or to the public without restriction from another source.

Protected Distribution System (PDS) – 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 through an area of lesser classification or control.

Pro

Protection Philosophy – Informal description of the overall design of an information system delineating each of the protection mechanisms employed. Combination of formal and informal techniques, appropriate to the evaluation class, used to show the mechanisms are adequate to enforce the security policy.

Protection Profile – Common Criteria specification that represents an implementation-independent set of security requirements for a category of Target of Evaluations (TOE) that meets specific consumer needs.

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.

Protective Packaging – Packaging techniques for COMSEC material that discourage penetration, reveal a penetration has occurred or was attempted, or inhibit viewing or copying of keying material prior to the time it is exposed for use.

Protective Technologies – Special tamper-evident features and materials employed for the purpose of detecting tampering and deterring attempts to compromise, modify, penetrate, extract, or substitute information processing equipment and keying material.

Protocol – Set of rules and formats, semantic and syntactic, permitting information systems to exchange information.

Protocol Data Unit – Is a unit of data specified in a protocol and consisting of protocol information and, possibly, user data.

Protocol Entity – Entity that follows a set of rules and formats (semantic and syntactic) that determines the communication behavior of other entities.

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, a Hyper Text Transfer Protocol (HTTP) proxy used for Web access, and a Simple Mail Transfer Protocol (SMTP) proxy used for email; 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.

> Note: This effectively closes the straight path between the internal and external networks, making it more difficult for an attacker to obtain internal addresses and other details of the organization's internal network. Proxy servers are available for common Internet services; for example, a Hyper Text Transfer Protocol (HTTP) proxy used for Web access, and a Simple Mail Transfer Protocol (SMTP) proxy used for email.

Proxy Agent – A software application running on a firewall or on a dedicated proxy server that is capable of filtering a protocol and routing it between the interfaces of the device.

Proxy Server – Is a server that services the requests of its clients by forwarding those requests to other servers.

Pseudonym – A false name.

1. A subscriber name that has been chosen by the subscriber that is not verified as meaningful by identity proofing.
2. An assigned identity that is used to protect an individual's true identity.

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.

Public Domain Software – Software not protected by copyright laws of any nation that may be freely used without permission of, or payment to, the creator, and that carries no warranties from, or liabilities to the creator.

Public Key – Is the public part of an asymmetric key pair that is typically used to verify signatures or encrypt data.

Public Key – Is a cryptographic key, used with a public key cryptographic algorithm that 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, for example, to:

1. Verify a digital signature that is signed by the corresponding private key,
2. Encrypt keys that can be decrypted by the corresponding private key, or
3. Compute a shared secret during a key-agreement transaction.

Public Key – 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. A cryptographic key used with a public key cryptographic algorithm that is uniquely associated with an entity and that may be made public; A cryptographic key that may be widely published and is used to enable the operation of an asymmetric cryptography scheme. This key is mathematically linked with a corresponding private key. Typically, a public key can be used to encrypt, but not decrypt, or to validate a signature, but not to sign.

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.

Public Key Certificate – A digital document issued and digitally signed by the private key of a Certificate 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; 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); 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.

Public Key Cryptography – Is an encryption system that uses a public-private key pair for encryption and/or digital signature.

Public Key Enabling (PKE) – The incorporation of the use of certificates for security services such as authentication, confidentiality, data integrity, and non-repudiation.

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.

Public Key Infrastructure – 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; A Framework that is established to issue, maintain, and revoke public key certificates; A support service to the PIV system that provides the cryptographic keys needed to perform digital signature-based identity verification and to protect communications and storage of sensitive verification system data within identity cards and the verification system; The framework and services that provide for the generation, production, distribution, control, accounting, and destruction of public key certificates. Components include the personnel, 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, recover, and revoke public key certificates.

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."

Purge – Rendering sanitized data unrecoverable by laboratory attack methods.

Q

Quadrant – Short name referring to technology that provides tamper-resistant protection to cryptographic equipment.

Qualitative Assessment – Use of a set of methods, principles, or rules for assessing risk based on nonnumeric categories or levels.

Quality of Service – The measurable end-to-end performance properties of a network service, which can be guaranteed in advance by a Service-Level Agreement between a user and a service provider, so as to satisfy specific customer application requirements. Note: These properties may include throughput (bandwidth), transit delay (latency), error rates, priority, security, packet loss, packet jitter, etc.

Quantitative Assessment – Use of a set of methods, principles, or rules for assessing risks based on the use of numbers where the meanings and proportionality of values are maintained inside and outside the context of the assessment.

Quarantine – Store files containing malware in isolation for future disinfection or examination.

R

Radio Frequency Identification (RFID) – a form of automatic identification and data capture (AIDC) that uses electric or magnetic fields at radio frequencies to transmit information.

Random Bit Generator (RBG) – A device or algorithm that outputs a sequence of binary bits that appears to be statistically independent and unbiased. An RBG is either a DRBG or an NRBG.

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; 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.

Randomizer – is an analog or digital source of unpredictable, unbiased, and usually independent bits. Randomizers can be used for several different functions, including key generation or to provide a starting state for a key generator.

Ranges Header Field Memory Exhaustion - The vulnerability is due to an error while pursing the Ranges Header Field which causes the program to consume excessive resources. A remote, unauthenticated attacker can exploit this vulnerability by sending a specially request to the vulnerable server causing it to become unresponsive.

Read – Fundamental operation in an information system that results only in the flow of information from an object to a subject.

Read Access – Permission to read information in an information system.

Really Simple Syndication (RSS) - which is an internet based technology that allows the distribution of Web content through an RSS reader. Using RSS, news articles, press releases, and other content can be gathered together and distributed via news feeds on an RSS server connected to the internet.

Real-Time Reaction – Immediate response to a penetration attempt that is detected and diagnosed in time to prevent access.

Real Time Streaming Protocol (RTSP) - is an official Internet standard (*RFC* 2326) for delivering and receiving streams of data such as audio and video. The standard allows for both real-time ("live") streams of data and streams from stored data.

Recipient Usage Period – Is the period of time during the crypto period of a symmetric key when protected information is processed.

Reciprocity – Mutual agreement among participating enterprises to accept each other's security assessments in order to reuse information system resources and/or to accept each other's assessed security posture in order to share information. Mutual agreement among participating organizations to accept each other's security assessments in order to reuse information system resources and/or to accept each other's assessed security posture in order to share information.

Records – The recordings (automated and/or manual) of evidence of activities performed or results achieved (e.g., forms, reports, test results), which serve as a basis for verifying that the organization and the information system are performing as intended. Also used to refer to units of related data fields (i.e., groups of data fields that can be accessed by a program and that contain the complete set of information on particular items); All books, papers, maps, photographs, machine-readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States government under federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the government or because of the informational value of the data in them.

Recovery Point Objective – The point in time to which data must be recovered after an outage.

Recovery Procedures – Actions necessary to restore data files of an information system and computational capability after a system failure.

Recovery Time Objective – The overall length of time an information system's components can be in the recovery phase before negatively impacting the organization's mission or mission/business functions.

RED – In cryptographic systems, refers to information or messages that contain sensitive or classified information that is not encrypted. See also BLACK.

Red Signal – Any electronic emission (e.g., plain text, key, key stream, sub key stream, initial fill, or control signal) that would divulge national security information if recovered.

Red Team – A group of people authorized and organized to emulate a potential adversary's attack or exploitation capabilities against an enterprise's security posture. The Red Team's objective is to improve enterprise Information Assurance by demonstrating the impacts of successful attacks and by demonstrating what works for the defenders (i.e., the Blue Team) in an operational environment.

Red Team Exercise – An exercise, reflecting real-world conditions, that is conducted as a simulated adversarial attempt to compromise organizational missions and/or business processes to provide a comprehensive assessment of the security capability of the information system and organization.

Red/Black Concept – Separation of electrical and electronic circuits, components, equipment, and systems that handle unencrypted information (Red), in electrical form, from those that handle encrypted information (Black) in the same form.

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

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. The process through which an Applicant applies to become a Subscriber of a CSP and an RA validates the identity of the Applicant on behalf of the CSP.

Registration Authority (RA) – Is 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).

Registration Authority (RA) – Organization responsible for assignment of unique identifiers to registered objects.

Rekey – To change the value of a cryptographic key that is being used in a cryptographic system/application.

Rekey (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.

Release Prefix – Prefix appended to the short title of U.S.-produced keying material to indicate its foreign releasability. "A" designates material that is releasable to specific allied nations, and "U.S." designates material intended exclusively for U. S. use.

RELURL - One of two basic kinds of uniform resource identifiers (URIs). It is a string of characters that gives a resource's file name (such as parking. html) but does not specify its type or exact location.

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

Remanence – Residual information remaining on storage media after clearing. See Magnetic Remanence and Clearing.

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

Remediation Plan – Is 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.

Remote Access – Access to an organizational information system by a user (or an information system acting on behalf of a user) communicating through an external network (e.g., the Internet; Access by users (or information systems) communicating external to an information system security perimeter; The ability for an organization's users to access its nonpublic computing resources from external locations other than the organization's facilities.

Remote Desktop Protocol (RDP) - The communication protocol used to provide remote viewing and control of Microsoft Windows computers and applications.
For additional information

Remote Diagnostics/Maintenance – Maintenance activities conducted by authorized individuals communicating through an external network (e.g., the Internet).

Remote Maintenance – Maintenance activities conducted by individuals communicating external to an information system security perimeter; Maintenance activities conducted by individuals communicating through an external network (e.g., the Internet).

Remote Rekeying – Procedure by which a distant crypto-equipment is rekeyed electrically. See: Automatic Remote Rekeying and Manual Remote Rekeying.

Removable Media – Portable electronic storage media such as magnetic, optical, and solid-state devices, which can be inserted into and removed from a computing device, and that, is used to store text, video, audio, and image information. Such devices have no independent processing capabilities. Examples include hard disks, floppy disks, zip drives, compact disks (CDs), thumb drives, pen drives, and similar USB storage devices.

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.

Repair Action – NSA-approved change to a COMSEC end-item that does not affect the original characteristics of the end-item and is provided for optional application by holders. Repair actions are limited to minor electrical and/or mechanical improvements to enhance operation, maintenance, or reliability. They do not require an identification label, marking, or control but must be fully documented by changes to the maintenance manual.

Replay Attacks – An attack that involves the capture of transmitted authentication or access control information and its subsequent retransmission with the intent of producing an unauthorized effect or gaining unauthorized access.

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

Reserve Keying Material – Key held to satisfy unplanned needs. See Contingency Key.

Residual Risk – The remaining potential risk after all IT security measures are applied. There is a residual risk associated with each threat; Portion of risk remaining after security measures have been applied.

Residue – Data left in storage after information-processing operations are complete, but before degaussing or overwriting has taken place.

Resilience – The ability to quickly adapt and recover from any known or unknown changes to the environment through holistic implementation of risk management, contingency, and continuity planning; The ability to continue to: (i) operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities; and (ii) recover to an effective operational posture in a time frame consistent with mission needs.

Resource Definition Framework (RDF) - A set of rules (a sort of language) for creating descriptions of information, especially information available on the *World Wide Web*. RDF could be used to describe a collection of books, or artists, or a collection of *web pages* as in the *RSS* data format which uses RDF to create machine-readable summaries of web sites. RDF is also used in *XPFE* applications to define the relationships between different collections of elements, for example RDF could be used to define the relationship between the data in a database and the way that data is displayed to a user.

Resource Encapsulation – Method by which the reference monitors mediates accesses to an information system resource. Resource is protected and not directly accessible by a subject; Satisfies requirement for accurate auditing of resource usage.

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

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.

Responsibility to Provide – Is an information distribution approach whereby relevant essential information is made readily available and discoverable to the broadest possible pool of potential users.

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

RFID – See: Radio Frequency Identification.

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

Ris

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

Risk Analysis – Is 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; Examination of information to identify the risk to an information system.

Risk Assessment – The process of identifying risks to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation, arising through the operation of an information system; Part of risk management, incorporates threat and vulnerability analyses and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis; The process of identifying, prioritizing, and estimating risks. This includes determining the extent to which adverse circumstances or events could impact an enterprise. Uses the results of threat and vulnerability assessments to identify risk to organizational operations and evaluates those risks in terms of likelihood of occurrence and impacts if they occur. The product of a risk assessment is a list of estimated potential impacts and unmitigated vulnerabilities. Risk assessment is part of risk management and is conducted throughout the Risk Management Framework (RMF).

Risk Assessment Methodology – A risk assessment process, together with a risk model, assessment approach, and analysis approach.

Risk Assessment Report – The report which contains the results of performing a risk assessment or the formal output from the process of assessing risk.

Risk Assessor –The individual, group, or organization responsible for conducting a risk assessment.

Risk Executive -(or Risk Executive Function) An individual or group within an organization that helps to ensure that: (i) security risk-related considerations for individual information systems, to include the authorization decisions for those systems, are viewed from an organization-wide perspective with regard to the overall strategic goals and objectives of the organization in carrying out its missions and business functions; and (ii) managing risk from individual information systems is consistent across the organization, reflects organizational risk tolerance, and is considered along with other organizational risks affecting mission/business success.

Risk Management – The process of managing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system, and includes: (i) the conduct of a risk assessment; (ii) the implementation of a risk mitigation strategy; and (iii) employment of techniques and procedures for the continuous monitoring of the security state of the information system.

Risk Management – 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.

Risk Management – Is 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.

Risk Management Framework – A structured approach used to oversee and manage risk for an enterprise.

Risk Mitigation – Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process.

Risk Model – Is a key component of a risk assessment methodology (in addition to assessment approach and analysis approach) that defines key terms and assessable risk factors.

Risk Monitoring – Maintaining ongoing awareness of an organization's risk environment, risk management program, and associated activities to support risk decisions.

Risk Response – Is accepting, avoiding, mitigating, sharing, or transferring risk to organizational operations (i.e., mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation.

Risk Response Measure – A specific action taken to respond to an identified risk.

Risk Tolerance – The level of risk an entity is willing to assume in order to achieve a potential desired result; the defined impacts to an enterprise's information systems that an entity is willing to accept.

Risk-Adaptable Access Control (RAdAC) - a form of access control that uses an authorization policy that takes into account operational need, risk, and heuristics.

Robust Security Network (RSN) – A wireless security network that only allows the creation of Robust Security Network Associations (RSNAs).

Robust Security Network Association (RSNA) – A logical connection between communicating IEEE 802.11 entities established through the IEEE 802.11i key management scheme, also known as the four-way handshake.

Robustness – The ability of an Information Assurance entity to operate correctly and reliably across a wide range of operational conditions, and to fail gracefully outside of that operational range.

Rogue Device –An unauthorized node on a network.

Role – A group attribute that ties membership to function. When an entity assumes a role, the entity is given certain rights that belong to that role. When the entity leaves the role, those rights are removed. The rights given are consistent with the functionality that the entity needs to perform the expected tasks.

Role-Based Access Control (RBAC) – A model for controlling access to resources where permitted actions on resources are identified with roles rather than with individual subject identities; Access control based on user roles (i.e., a collection of access authorizations a user receives based on an explicit or implicit assumption of a given role). Role permissions may be inherited through a role hierarchy and typically reflect the permissions needed to perform defined functions within an organization. A given role may apply to a single individual or to several individuals.

Root - Refers to the most privileged access possible on a computer system. With root access, one can create, delete (or corrupt) anything on the system.

Root Cause Analysis –A principle-based, systems approach for the identification of underlying causes associated with a particular set of risks.

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.

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; a piece of software that can be installed and hidden on the victim computer without the user's knowledge. It may be included in a larger software package or installed by an attacker who has been able to take advantage of vulnerability on the victim machine. Rootkits are not necessarily malicious, but they may hide malicious activities. Attackers may be able to access information, monitor user actions, modify programs, or perform other functions on the targeted computer without being detected

Root Kit - A collection of programs that enable administrator-level access to a computer or computer network. Typically, a hacker installs a root kit on a computer after first obtaining user-level access. Once the root kit is installed, it allows the attacker to mask intrusion and gain privileged access.

Roshal Archive (RAR) - A compressed file format similar in use to the more popular ZIP format. It is used to conserve storage and network resources and simplifies the movement of large sets of files. Optional encryption is available using the NIST Advanced Encryption Standard algorithm. Just as ZIP archives are created with software such as WinZip.

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.

Router - A hardware device that connects two or more networks and routes incoming data packets to the appropriate network. Many Internet Service Providers (ISPs) provide these devices to their customers, and they often contain firewall protections.

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; 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. Also known as discretionary access control (DAC).

Rules of Engagement (ROE) – Detailed guidelines and constraints regarding the execution of information security testing. The ROE is established before the start of a security test, and gives the test team authority to conduct defined activities without the need for additional permissions.

Rule set – A table of instructions used by a controlled interface to determine what data is allowable and how the data is handled between interconnected systems. A set of directives that govern the access control functionality of a firewall. The firewall uses these directives to determine how packets should be routed between its interfaces.

S

S-box – Nonlinear 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.

Safeguarding Statement – Statement affixed to a computer output or printout that states the highest classification being processed at the time the product was produced and requires control of the product, at that level, until determination of the true classification by an authorized individual.

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.

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.

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. A restricted, controlled execution environment that prevents potentially malicious software, such as mobile code, from accessing any system resources except those for which the software is authorized.

Sanitization – Process to remove information from media such that information recovery is not possible. It includes removing all labels, markings, and activity logs; a general term referring to the actions taken to render data written on media unrecoverable by both ordinary and, for some forms of sanitization, extraordinary means.

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

Scareware- fake security software warnings. This type of scam can be particularly profitable for cyber criminals, as many users believe the pop-up warnings telling them their system is infected and are lured into downloading and paying for the special software to "protect" their system.

Scatternet – A chain of piconets created by allowing one or more Bluetooth devices to each be a slave in one piconet and act as the master for another piconet simultaneously. A scatternet allows several devices to be networked over an extended distance.

Scavenging – Searching through object residue to acquire data.

Scoping Guidance – A part of tailoring guidance providing organizations with specific policy/regulatory-related, technology-related, system component allocation-related, operational/environmental-related, and physical infrastructure-related, public access-related, scalability-related, common control-related, and security objective-related considerations on the applicability and implementation of individual security controls in the security control baseline; 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.

Script- Is a file containing active content -- for example, commands or instructions to be executed by the computer.

Script Kiddies - Unskilled attackers who do not have the ability to discover new vulnerabilities or write exploit code, and are dependent on the research and tools from others. Their goal is achievement. Their sub-goals are to gain access and deface web pages.

Search Engine- A program that searches documents or indexes of documents for specified words or phrases and returns a list of the documents where those items were found.

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 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. A cryptographic key that is used with a symmetric cryptographic algorithm that is uniquely associated with one or more entities and is not 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.

Secret Key – A cryptographic key that must be protected from unauthorized disclosure to protect data encrypted with the key. The use of the term "secret" in this context does not imply a classification level; rather, the term implies the need to protect the key from disclosure or substitution; 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 or substitution; 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.

Secret Key (symmetric) Cryptographic Algorithm – A cryptographic algorithm that uses a single secret key for both encryption and decryption; A cryptographic algorithm that uses a single key (i.e., a secret key) for both encryption and decryption.

Secret Seed – A secret value used to initialize a pseudorandom number generator.

Secure Communication Protocol – A communication protocol that provides the appropriate confidentiality, authentication, and content-integrity protection.

Secure Communications – Telecommunications deriving security through use of NSA-approved products and/or Protected Distribution Systems.

Secure DNS (SECDNS) – Configuring and operating DNS servers so that the security goals of data integrity and source authentication are achieved and maintained.

Secure Erase – An overwrite technology using firmware-based process to overwrite a hard drive. Is a drive command defined in the ANSI ATA and SCSI disk drive interface specifications, which runs inside drive hardware. It completes in about 1/8 the time of 5220 block erasure.

Secure Hash Algorithm (SHA) – A hash algorithm with the property that is computationally infeasible 1) to find a message that corresponds to a given message digest, or 2) to find two different messages that produce the same message digest.

Secure Hash Standard – This Standard specifies secure hash algorithms -SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224 and SHA-512/256 -for computing a condensed representation of electronic data (message). When a message of any length less than 264 bits (for SHA-1, SHA-224 and SHA-256) or less than 2128 bits (for SHA-384, SHA-512, SHA-512/224 and SHA-512/256) is input to a hash algorithm, the result is an output called a message digest. The message digests range in length from 160 to 512 bits, depending on the algorithm. Secure hash algorithms are typically used with other cryptographic algorithms, such as digital signature algorithms and keyed-hash message authentication codes, or in the generation of random numbers (bits). The hash algorithms specified in this Standard are called secure because, for a given algorithm, it is computationally infeasible 1) to find a message that corresponds to a given message digest, or 2) to find two different messages that produce the same message digest. Any changes to a message will, with a very high probability, result in a different message digests. This will result in a verification failure when the secure hash algorithm is used with a digital signature algorithm or a keyed-hash message authentication algorithm. Specification for a secure hash algorithm that can generate a condensed message representation called a message digest.

Secure Socket Layer (SSL) – A protocol used for protecting private information during transmission via the Internet.

> Note: 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:"

Secure State – Condition in which no subject can access any object in an unauthorized manner.

Secure Subsystem – subsystem containing its own implementation of the reference monitor concept for those resources it controls. Secure subsystem must depend on other controls and the base operating system for the control of subjects and the more primitive system objects.

Secure/Multipurpose Internet Mail Extensions (S/MIME) – Is 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).

Security – A condition that results from the establishment and maintenance of protective measures that enable an enterprise to perform its mission or critical functions despite risks posed by threats to its use of information systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the enterprise's risk management approach.

Security Assertion Markup Language (SAML) – An XML-based security specification developed by the Organization for the Advancement of Structured Information Standards (OASIS) for exchanging authentication (and authorization) information between trusted entities over the Internet; A framework for exchanging authentication and authorization information. Security typically involves checking the credentials presented by a party for authentication and authorization. SAML standardizes the representation of these credentials in an XML format called "assertions," enhancing the interoperability between disparate applications. A protocol consisting of XML-based request and response message formats for exchanging security information, expressed in the form of assertions about subjects, between online business partners.

Security Association – A relationship established between two or more entities to enable them to protect data they exchange.

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; An abstraction representing the basic properties or characteristics of an entity with respect to safeguarding information; typically associated with internal data structures (e.g., records, buffers, files) within the information system which are used to enable the implementation of access control and flow control policies; reflect special dissemination, handling, or distribution instructions; or support other aspects of the information security policy.

Security Automation Domain – Is an information security area that includes a grouping of tools, technologies, and data.

Security Banner – Is a banner at the top or bottom of a computer screen that states the overall classification of the system in large, bold type; also can refer to the opening screen that informs users of the security implications of accessing a computer resource.

Security Categorization – Is the process of determining the security category for information or an information system. See Security Category; The process of determining the security category for information or an information system. Security categorization methodologies are described in CNSS Instruction 1253 for national security systems and in FIPS 199 for other than national security systems.

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. 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, individuals, other organizations, and the Nation.

Security Concept of Operations –A security-focused description of an information system, its operational policies, classes of users, interactions between the system and its users, and the system's contribution to the operational mission.

Security Content Automation Protocol (SCAP) – A method for using specific standardized testing methods to enable automated vulnerability management, measurement, and policy compliance evaluation against a standardized set of security requirements.

Security Control Assessment – The testing and/or evaluation of the management, operational, and technical security controls in an information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system; The testing and/or evaluation of the management, operational, and technical security controls 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 and/or enterprise.

Security Control Assessor – The individual, group, or organization responsible for conducting a security control assessment.

Security Control Effectiveness – The measure of correctness of implementation (i.e., how consistently the control implementation complies with the security plan) and how well the security plan meets organizational needs in accordance with current risk tolerance.

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. Statements of security capability to: (i) build in additional, but related, functionality to a security control; and/or (ii) increase the strength of the control.

Security Control Inheritance – A situation in which an information system or application receives protection from security controls (or portions of security controls) that are developed, implemented, assessed, authorized, and monitored by entities other than those responsible for the system or application; entities either internal or external to the organization where the system or application resides.
See Common Control.

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.

Security Controls Baseline – The set of minimum security controls defined for a low-impact, moderate-impact, or high-impact information system.

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

Security Domain – Is a collection of entities to which applies a single security policy executed by a single authority; A domain that implements a security policy and is administered by a single authority.

Security Engineering – An interdisciplinary approach and means to enable the realization of secure systems. It focuses on defining customer needs, security protection requirements, and required functionality early in the systems development life cycle, documenting requirements, and then proceeding with design, synthesis, and system validation while considering the complete problem.

Security Event and Information Management (SEIM) – Centralized collection and management of security event records from many different systems such as firewalls, IDS/IPS, antivirus software, authentication systems, etc. SEIMs may provide complex multifactor rules to alert on patterns of behavior not easily identifiable by one of the component systems alone.

Security Fault Analysis (SFA) – An assessment usually performed on information system hardware, to determine the security properties of a device when hardware fault is encountered.

Security Features Users Guide (SFUG) - Guide or manual explaining how the security mechanisms in a specific system work.

Security Filter – Is a secure subsystem of an information system that enforces security policy on the data passing through it.

Security Functions – The hardware, software, and/or firmware of the information system responsible for enforcing the system security policy and supporting the isolation of code and data on which the protection is based.

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

Security Impact Analysis – The analysis conducted by an organizational official to determine the extent to which changes to the information system have affected the security state of the system.

Security Information and Event Management (SIEM) Tool – Is an application that provides the ability to gather security data from information system components and present that data as actionable information via a single interface.

Security Inspection – Examination of an information system to determine compliance with security policy, procedures, and practices.

Security Kernel – Hardware, firmware, and software elements of a trusted computing base implementing the reference monitor concept. Security kernel must mediate all accesses, be protected from modification, and be verifiable as correct.

Security Label – The means used to associate a set of security attributes with a specific information object as part of the data structure for that object; a marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource.

Security Level – Is 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.

Security Management Dashboard – A tool that consolidates and communicates information relevant to the organizational security posture in near real-time to security management stakeholders.

Security Marking – Is a human-readable information affixed to information system components, removable media, or output indicating the distribution limitations, handling caveats, and applicable security markings.

Security Markings – Human-readable indicators applied to a document, storage media, or hardware component to designate security classification, categorization, and/or handling restrictions applicable to the information contained therein. For intelligence information, these could include compartment and sub-compartment indicators and handling restrictions.

Security Mechanism – A device designed to provide one or more security services usually rated in terms of strength of service and assurance of the design.

Security Net Control Station – Is a management system overseeing and controlling implementation of network security policy.

Security Objective – Confidentiality, integrity, or availability.

Security Perimeter – A physical or logical boundary that is defined for a system, domain, or enclave, within which particular security policy or security architecture is applied.

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

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

Security Posture – The security status of an enterprise's networks, information, and systems based on IA resources (e.g., people, hardware, software, policies) and capabilities in place to manage the defense of the enterprise and to react as the situation changes.

Security Program Plan – Is a formal document that provides an overview of the security requirements for an organization-wide information security program and describes the program management security controls and common security controls in place or planned for meeting those requirements.

Security Range – Is the highest and lowest security levels that are permitted in or on an information system, system component, subsystem, or network.

Security-Relevant Change – Any change to a system's configuration, environment, information content, functionality, or users which has the potential to change the risk imposed upon its continued operations.

Security-Relevant Event – An occurrence (e.g., an auditable event or flag) considered to have potential security implications to the system or its environment that may require further action (noting, investigating, or reacting).

Security-Relevant Information – Any information within the information system that can potentially impact the operation of security functions in a manner that could result in failure to enforce the system security policy or maintain isolation of code and data.

Security Requirements - 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.

Security Requirements Baseline – Description of the minimum requirements necessary for an information system to maintain an acceptable level of risk.

Security Requirements Traceability Matrix (SRTM) – Matrix that captures all security requirements linked to potential risks and addresses all applicable C&A requirements. It is, therefore, a correlation statement of a system's security features and compliance methods for each security requirement.

Security Safeguards – Protective measures and controls prescribed to meet the security requirements specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices.

Security Service – Is a capability that supports one, or many, of the security goals. Examples of security services are key management, access control, and authentication; A capability that supports one, or more, of the security requirements (Confidentiality, Integrity, Availability). Examples of security services are key management, access control, and authentication.

Security Specification – Detailed description of the safeguards required to protect an information system.

Security Strength – A measure of the computational complexity associated with recovering certain secret and/or security-critical information concerning a given cryptographic algorithm from known data (e.g. plaintext/ciphertext pairs for a given encryption algorithm). A number associated with the amount of work (that is, the number of operations) that is required to break a cryptographic algorithm or system; sometimes referred to as a security level.

Security Tag – Is an information unit containing a representation of certain security-related information (e.g., a restrictive attribute bit map).

Security Target – Is a common Criteria specification that represents a set of security requirements to be used as the basis of an evaluation of an identified Target of Evaluation (TOE).

Security Test & Evaluation (ST&E) – Examination and analysis of the safeguards required to protect an information system, as they have been applied in an operational environment, to determine the security posture of that system.

Security Testing – Process to determine that an information system protects data and maintains functionality as intended.

Seed Key – Initial key used to start an updating or key generation process.

Semi-Quantitative Assessment – Use of a set of methods, principles, or rules for assessing risk based on bins, scales, or representative numbers whose values and meanings are not maintained in other contexts.

Sensitive Compartmented Information (SCI) – Classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems established by the Director of National Intelligence.

Sensitive Compartmented Information Facility (SCIF) – Accredited area, room, or group of rooms, buildings, or installation where SCI may be stored, used, discussed, and/or processed.

Sensitivity – A measure of the importance assigned to information by its owner, for the purpose of denoting its need for protection.

Sensitivity Label – Information representing elements of the security label(s) of a subject and an object. Sensitivity labels are used by the trusted computing base (TCB) as the basis for mandatory access control decisions. See Security Label.

Server - A computer, or a software package, that provides a specific kind of service to *client* software running on other computers. The term can refer to a particular piece of software, such as a *WWW* server, or to the machine on which the software is running, e.g. "Our mail server is down today, that's why e-mail isn't getting out."
A single server machine can (and often does) have several different server software packages running on it, thus providing many different servers to *clients* on the *network*. Sometimes server software is designed so that additional capabilities can be added to the main program by adding small programs known as *servlets*.

Serv-Si

Server Servers - are powerful computers or processes dedicated to managing disk drives (file servers), printers (print servers), or network traffic (network servers).

Service-Level Agreement – Defines the specific responsibilities of the service provider and sets the customer expectations.

Servlet - A small computer program designed to be added capabilities to a larger piece of *server* software. Common examples are "Java servlets", which are small programs written in the *Java* language and which are added to a *web* server. Typically a web server that uses Java servlets will have many of them, each one designed to handle a very specific situation, for example one servlet will handle adding items to a "shopping cart", while a different servlet will handle deleting items from the "shopping cart."

Session - A virtual connection between two hosts by which network traffic is passed.

Shared Secret – A secret used in authentication that is known to the Claimant and the Verifier.

Shielded Enclosure – Room or container designed to attenuate electromagnetic radiation, acoustic signals, or emanations.

Short Title – Identifying combination of letters and numbers assigned to certain COMSEC materials to facilitate handling, accounting, and controlling.

Side Channel Attack - An attack on a cryptographic system whereby data from other dependent systems is measured from which inferences can be made. Power consumption, timing analysis and acoustic emanations are example data sources for side-channel attacks.

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; A recognizable, distinguishing pattern. See also Attack Signature or Digital Signature.

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.

Signature Generation – Uses a digital signature algorithm and a private key to generate a digital signature on data; the process of using a digital signature algorithm and a private key to generate a digital signature on data.

Signature Validation – Is the (mathematical) verification of the digital signature and obtaining the appropriate assurances (e.g., public key validity, private key possession, etc.).

Signature Verification – Is the use of a digital signature algorithm and a public key to verify a digital signature on data; the process of using a digital signature algorithm and a public key to verify a digital signature on data.

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

Single Point Keying – Means of distributing key to multiple, local crypto equipment or devices from a single fill point.

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

Situational Awareness – Is within a volume of time and space, the perception of an enterprise's security posture and its threat environment; the comprehension/meaning of both taken together (risk); and the projection of their status into the near future.

Skimming – The unauthorized use of a reader to read tags without the authorization or knowledge of the tag's owner or the individual in possession of the tag.

Slowloris - Is a piece of software to take down a web server with minimal band width and side effects unrelated services and ports by trying to keep many connections to the target web server open and hold them open as long as possible

Smart Card – A credit card-sized card with embedded integrated circuits that can store, process, and communicate information.

Sniffer – See: Passive Wiretapping.

Social Engineering – An attempt to trick someone into revealing information (e.g., a password) that can be used to attack systems or networks. A general term for attackers trying to trick people into revealing sensitive information or performing certain actions, such as downloading and executing files that appear to be benign but are actually malicious; The process of attempting to trick someone into revealing information (e.g., a password)

Social Engineering - A euphemism for non-technical or low-technology means—such as lies, impersonation, tricks, bribes, blackmail and threats—used to attack information systems.

Social Network Attacks - Social network attacks are major sources of attacks because of the volume of users and the amount of personal information that is posted. Users' inherent trust in their online friends is what makes these networks a prime target. For example, users may be prompted to follow a link on someone's page, which could bring users to a malicious website.

Software – Computer programs and associated data that may be dynamically written or modified during execution.

Software Assurance – Level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at any time during its life cycle, and that the software functions in the intended manner.

Software System Test and Evaluation Process – Process that plans, develops, and documents the qualitative/quantitative demonstration of the fulfillment of all baseline functional performance, operational, and interface requirements.

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 Code – Is the code for a software program, as written by the programmer, which is the intellectual property of the software developer.

Spam – The abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages; unsolicited bulk commercial email messages; Electronic junk mail or the abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages.

Spam - Unwanted, unsolicited email from someone you don't know. Often sent in an attempt to sell you something or get you to reveal personal information.

Spam Filtering Software – A program that analyzes emails to look for characteristics of spam, and typically places messages that appear to be spam in a separate email folder.

Spear phishing - A targeted phishing attack against a select group of victims, usually belonging to a single company, school, industry, etc; A targeted phishing attack against a select group of victims, usually belonging to a single company, school, industry, etc. "Spearphishing" is commonly used to refer to any targeted email attack, not limited to phishing.

Special Access Program (SAP) – A program established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level.

Special Access Program Facility (SAPF) – Facility formally accredited by an appropriate agency in accordance with DCID 6/9 in which SAP information may be processed.

Special Character – Is any non-alphanumeric character that can be rendered on a standard American-English keyboard. Use of a specific special character may be application-dependent.

Specification – An assessment object that includes document-based artifacts (e.g., policies, procedures, plans, system security requirements, functional specifications, and architectural designs) associated with an information system.

Spider - A computer program that automatically retrieves Web documents. They are often used to feed pages to search engines for indexing; also known as a Web crawler.

Spillage – Security incident that results in the transfer of classified or CUI information onto an information system not accredited (i.e., authorized) for the appropriate security level.

Split Knowledge – A procedure by which a cryptographic key is split into n multiple key components, individually providing no knowledge of the original key, which can be subsequently combined to recreate the original cryptographic key. If knowledge of k (where k is less than or equal to n) components is required to construct the original key, then knowledge of any k-1 key components provides no information about the original key other than, possibly, its length.

Split Knowledge – 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.

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

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.
3. Faking the sending address of a transmission to gain illegal entry into a secure system. Impersonating, masquerading, piggybacking, and mimicking are forms of spoofing.
4. The deliberate inducement of a user or resource to take incorrect action

Spoofing - Masquerading so that a trusted IP address is used instead of the true IP address. A technique used by hackers as a means of gaining access to a computer system.

Spread Spectrum – Telecommunications techniques in which a signal is transmitted in a bandwidth considerably greater than the frequency content of the original information. Frequency hopping, direct sequence spreading, time scrambling, and combinations of these techniques are forms of spread spectrum.

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.

Spyware - Software that uses your Internet connection to send personally identifiable information about you to a collecting device on the Internet. It is often packaged with software that you download voluntarily, so that even if you remove the downloaded program later, the spyware may remain.

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

Standard Generalized Markup Language (SGML) - Developed in 1986 SGML provides a rich set of rules for defining new data formats. A well-known example of using SGML is *XML*, which is a subset of SGML: The definition of XML is all of SGML minus a couple of dozen items. SGML is an International Standards Organization (ISO) standard: ISO 8879:1986.

Start-Up KEK - Key-encryption-key held in common by a group of potential communicating entities and used to establish ad hoc tactical networks.

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

Static Key – A key that is intended for use for a relatively long period of time and is typically intended for use in many instances of a cryptographic key establish scheme

Status Monitoring – Monitoring the information security metrics defined by the organization in the information security ISCM strategy.

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**;** The art, science, and practice of communicating in a way that hides the existence of the communication; The act of embedding messages within another message (often a picture or media file) such that the message is hidden from common view.

Storage Object – Object supporting both read and write accesses to an information system.

Strength of Mechanism (SoM) – Is a scale for measuring the relative strength of a security mechanism.

Striped Core – A network architecture in which user data traversing a core IP network is decrypted, filtered and re-encrypted one or more times.

Note: The decryption, filtering, and re-encryption are performed within a "Red gateway"; consequently, the core is "striped" because the data path is alternately Black, Red, and Black.

Strong Authentication – Is the requirement to use multiple factors for authentication and advanced technology, such as dynamic passwords or digital certificates, to verify an entity's identity.

Structured Query Language (SQL) - A type of programming language used to interact with a database. The language is used to both update and issue queries to the database; a specialized language for sending queries to databases. Most industrial-strength and many smaller database applications can be addressed using SQL. Each specific application will have its own slightly different version of SQL

implementing features unique to that application, but all SQL-capable databases support a common subset of SQL.

Example of an SQL statement is:

SELECT name,email FROM people_table WHERE contry='uk'

Structured Query Language (SQL) Injection – Is an attack that involves the alteration of a database search in a web-based application, which can be used to obtain unauthorized access to sensitive information in a database.

Stuxnet - A sophisticated computer attack discovered in July 2010 that targeted control systems used to operate industrial processes in the energy, nuclear and other critical sectors. It is designed to exploit a combination of vulnerabilities to gain access to its target and modify code to change the process. Stuxnet primarily targeted Siemens SCADA systems used in the Iranian uranium enrichment program.

Subassembly – Major subdivision of an assembly consisting of a package of parts, elements, and circuits that perform a specific function.

Subject – Generally an individual, process, or device causing information to flow among objects or changes to the system state. See Object; An active entity (generally an individual, process, or device) that causes information to flow among objects or changes the system state. See also Object.

Subject Security Level – Sensitivity label(s) of the objects to which the subject has both read and write access. Security level of a subject must always be dominated by the clearance level of the user associated with the subject.

Subordinate Certification Authority – 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.

Subscriber – A party who receives a credential or token from a CSP (Credentials Service Provider) and becomes a claimant in an authentication protocol; a party who receives a credential or token from a CSP (Credentials Service Provider).

Subsystem – A major subdivision or component of an information system consisting of information, information technology, and personnel that perform one or more specific functions.

Suite A – A specific set of classified cryptographic algorithms used for the protection of some categories of restricted mission-critical information.

Suite B – A specific set of cryptographic algorithms suitable for protecting national security systems and information throughout the U.S. government and to support interoperability with allies and coalition partners.

Superencryption – Process of encrypting encrypted information. Occurs when a message, encrypted off-line, is transmitted over a secured, online circuit, or when information encrypted by the originator is multiplexed onto a communications trunk, which is then bulk encrypted.

Superior Certification Authority – 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.

Supersession – Scheduled or unscheduled replacement of COMSEC material with a different edition.

Supervisory Control and Data Acquisition (SCADA) – Is a generic name for a computerized system that is capable of gathering and processing data and applying operational controls over long distances. Typical uses include power transmission and distribution and pipeline systems. SCADA was designed for the unique communication challenges (delays, data integrity, etc.) posed by the various media that must be used, such as phone lines, microwave, and satellite. Usually shared rather than dedicated; Networks or systems generally used for industrial controls or to manage infrastructure such as pipelines and power systems; a process control application or system that collects data from sensors and machines locally or in remote locations and sends them to a central computer for management and control.

Supplementation (Assessment Procedures) – The process of adding assessment procedures or assessment details to assessment procedures in order to adequately meet the organization's risk management needs.

Supply Chain – A system of organizations, people, activities, information, and resources, possibly international in scope, that provides products or services to consumers.
Supply Chain Attack – Attacks that allow the adversary to utilize implants or other vulnerabilities inserted prior to installation in order to infiltrate data, or manipulate information technology hardware, software, operating systems, peripherals (information technology products) or services at any point during the life cycle.

Suppression Measure – Action, procedure, modification, or device that reduces the level of, or inhibits the generation of, compromising emanations in an information system.

Surrogate Access – See Discretionary Access Control.

Syllabary – List of individual letters, combination of letters, or syllables, with their equivalent code groups, used for spelling out words or proper names not present in the vocabulary of a code. A syllabary may also be a spelling table.

Symmetric Digital Subscriber Line (SDSL) - A version of *DSL* where the upload speeds and download speeds are the same.

Symmetric Encryption Algorithm – Encryption algorithms using the same secret key for encryption and decryption.

Symmetric Key – Is 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.

Symmetric Key – Is a single cryptographic key that is used with a secret (symmetric) key algorithm.

Synchronous Crypto-Operation – Encryption algorithms using the same secret key for encryption and decryption.

System – See: Information System. Any organized assembly of resources and procedures united and regulated by interaction or interdependence to accomplish a set of specific functions.

System Administrator – Is a person who manages the technical aspects of a system. Information system, providing effective information system utilization, adequate security parameters, and sound implementation of established Information Assurance policy and procedures.

System Assets – Is any software, hardware, data, administrative, physical, communications, or personnel resource within an information system.

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.

System Development Methodologies – Methodologies developed through software engineering to manage the complexity of system development. Development methodologies include software engineering aids and high-level design analysis tools.

System High – Is the highest security level supported by an information system.

System High Mode – Information systems security mode of operation wherein each user, with direct or indirect access to the information system, its peripherals, remote terminals, or remote hosts, has all of the following: a. valid security clearance for all information within an information system; b. formal access approval and signed nondisclosure agreements for all the information stored and/or processed (including all compartments, sub compartments and/or special access programs); and c. valid need-to-know for some of the information contained within the information system.

System Indicator – Symbol or group of symbols in an off-line encrypted message identifying the specific cryptosystem or key used in the encryption.

System Integrity – Is 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. Attribute of an information system when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

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

System Low – Is the lowest security level supported by an information system.

System Of Records – A group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

System Owner – Person or organization having responsibility for the development, procurement, integration, modification, operation and maintenance, and/or final disposition of an information system.

System Profile – Detailed security description of the physical structure, equipment component, location, relationships, and general operating environment of an information system.

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; The formal document prepared by the information system owner (or common security controls owner for inherited controls) that provides an overview of the security requirements for the system and describes the security controls in place or planned for meeting those requirements. The plan can also contain as supporting appendices or as references, other key security-related documents such as a risk assessment, privacy impact assessment, system interconnection agreements, contingency plan, security configurations, configuration management plan, and incident response plan.

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, associated programs, and data.

Systems Security Engineering – See: Information Systems Security Engineering.

Systems Security Officer – See: Information Systems Security Officer.

System-Specific Security Control – A security control for an information system that has not been designated as a common security control or the portion of a hybrid control that is to be implemented within an information system.

T

T-1 - A *leased-line* connection capable of carrying data at 1,544,000 *bits*-per-second. At maximum theoretical capacity, a T-1 line could move a *megabyte* in less than 10 seconds. That is still not fast enough for full-screen, full-motion video, for which you need at least 10,000,000 bits-per-second. T-1 lines are commonly used to connect large *LAN*s to the *Internet*.

T-3 - A *leased-line* connection capable of carrying data at 44,736,000 bits-per-second. This is more than enough to do full-screen, full-motion video.

Tabletop Exercise – A discussion-based exercise where personnel with roles and responsibilities in a particular IT plan meet in a classroom setting or in breakout groups, to validate the content of the plan by discussing their roles during an emergency and their responses to a particular emergency situation. A facilitator initiates the discussion by presenting a scenario and asking questions based on the scenario.

Tactical Data –Information that requires protection from disclosure and modification for a limited duration as determined by the originator or information owner.

Tactical Edge – The platforms, sites, and personnel operating at lethal risk in a battle space or crisis environment characterized by 1) a dependence on information systems and connectivity for survival and mission success, 2) high threats to the operational readiness of both information systems and connectivity, and 3) users are fully engaged, highly stressed, and dependent on the availability, integrity, and transparency of their information systems.

Tailored Security Control Baseline– A set of security controls, resulting from the application of tailoring guidance, to the security control baseline. See Tailoring; a set of security controls resulting from the application of tailoring guidance to the security control baseline. See: Tailoring.

Tag - The term "tag" can be used as a noun or verb. As a noun, a tag is a basic element of the languages used to create web pages (*HTML*) and similar languages such as *XML*. Another, more recent meaning of tag is related to reader-created tags where blogs and other content (such as photos, music, etc.) may be "tagged" which means to assign a keyword, such as "politics" or "gardening", this enables searches for "all the blog postings in the past week that are tagged 'prenatal care'"

Target Of Evaluation (TOE) – In accordance with Common Criteria, an information system is part of a system or product, and all associated documentation that is the subject of a security evaluation.

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

Technical Reference Model (TRM) – A component-driven, technical framework that categorizes the standards and technologies to support and enable the delivery of service components and capabilities.

Technical Security Controls – 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.

Technical Vulnerability Information – Detailed description of a weakness to include the implementable steps (such as code) necessary to exploit that weakness

Telecommunications – Preparation, transmission, communication, or related processing of information (writing, images, sounds, or other data) by electrical, electromagnetic, electromechanical, electro-optical, or electronic means.

Telework – The ability for an organization's employees and contractors to perform work from locations other than the organization's facilities.

Telnet - The command and program used to *login* from one *Internet* site to another. The telnet command/program gets you to the login: prompt of another *host*.

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

TEMPEST Test – Laboratory or on-site test to determine the nature of compromising emanations associated with an information system.

TEMPEST Zone – Is a designated area within a facility where equipment with appropriate TEMPEST characteristics (TEMPEST zone assignment) may be operated.

Terminal - A device that allows you to send commands to a computer somewhere else. At a minimum, this usually means a keyboard and a display screen and some simple circuitry. Usually you will use terminal software in a personal computer - the software pretends to be (emulates) a physical terminal and allows you to type commands to a computer somewhere else.

Terminal Server- Is a special purpose computer that has places to plug in many *modems* on one side, and a connection to a *LAN* or *host* machine on the other side. Thus the terminal server does the work of answering the calls and passes the connections on to the appropriate *node*. Most terminal servers can provide *PPP* or *SLIP* services if connected to the *Internet*.

Test – A type of assessment method that is characterized by the process of exercising one or more assessment objects under specified conditions to compare actual with expected behavior, the results of which are used to support the determination of security control effectiveness over time.

Test Key – Key intended for testing of COMSEC equipment or systems.

Threat – 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 particular information system vulnerability.

Threat Analysis – Is the examination of threat sources against system vulnerabilities to determine the threats for a particular system in a particular operational environment.

Threat Assessment – Is a formal description and evaluation of threat to an information system; Process of formally evaluating the degree of threat to an information system or enterprise and describing the nature of the threat.

Threat Event – An event or situation that has the potential for causing undesirable consequences or impact.

Threat Monitoring – Analysis, assessment, and review of audit trails and other information collected for the purpose of searching out system events that may constitute violations of system security.

Threat Scenario – A set of discrete threat events, associated with a specific threat source or multiple threat sources, partially ordered in time.

Threat Shifting – Response from adversaries to perceived safeguards and/or countermeasures (i.e., security controls), in which the adversaries change some characteristic of their intent to do harm in order to avoid and/or overcome those safeguards/countermeasures.

Threat Source – The intent and method targeted at the intentional exploitation of vulnerability or a situation and method that may accidentally trigger vulnerability. Synonymous with Threat Agent; The intent and method targeted at the intentional exploitation of vulnerability or a situation and method that may accidentally exploit vulnerability.

Time Bomb – Is a resident computer program that triggers an unauthorized act at a predefined time.

Time-Compliance Date – Date by which a mandatory modification to a COMSEC end-item must be incorporated if the item is to remain approved for operational use.

Time-Dependent Password – Password that is valid only at a certain time of day or during a specified interval of time.

TOE Security Functions (TSF) – Set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TOE Security Policy (TSP).

TOE Security Policy (TSP) – Set of rules that regulate how assets are managed, protected, and distributed within the TOE.

Token – Something that the Claimant possesses and controls (typically a key or password) that is used to authenticate the Claimant's identity; something that the claimant possesses and controls (such as a key or password) that are used to authenticate a claim.

Top Level Domain (TLD) – Is the last (right-hand) part of a complete *Domain Name*. For example in the domain name www.matisse.net ".net" is the Top Level Domain. There are a large number of TLD's, for example .biz, .com, .edu, .gov, .info, .int, .mil, .net, .org, and a collection of two-letter TLD's corresponding to the standard two-letter country codes, for example, .us, .ca, .jp, etc.

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).

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.

Tradecraft Identity – An identity used for the purpose of work-related interactions that may or may not be synonymous with an individual's true identity.

Traditional INFOSEC Program – Program in which NSA acts as the central procurement agency for the development and, in some cases, the production of INFOSEC items. This includes the Authorized Vendor Program. Modifications to the INFOSEC end-items used in products developed and/or produced under these programs must be approved by NSA.

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; the analysis of patterns in communications for the purpose of gaining intelligence about a system or its users. It does not require examination of the content of the communications, which may or may not be decipherable. For example, an adversary may be able to detect a signal from a reader that could enable it to infer that a particular activity is occurring (e.g., a shipment has arrived, someone is entering a facility) without necessarily learning an identifier or associated data; Gaining knowledge of information by inference from observable characteristics of a data flow, even if the information is not directly available (e.g., when the data is encrypted). These characteristics include the identities and locations of the source(s) and destination(s) of the flow, and the flow's presence, amount, frequency, and duration of occurrence.

Traffic Encryption Key (TEK) – Key used to encrypt plain text or to Superencryption previously encrypted text and/or to decrypt cipher text.

Traffic-Flow Security (TFS) – Techniques to counter Traffic Analysis.

Traffic Padding – Generation of mock communications or data units to disguise the amount of real data units being sent.

Training (Information Security) – Training strives to produce relevant and needed (information) security skills and competencies.

Training Assessment – Is an evaluation of the training efforts.

Training Effectiveness – A measurement of what a given student has learned from a specific course or training event.

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.

Tranquility – Property whereby the security level of an object cannot change while the object is being processed by an information system.

Transmission – The state that exists when information is being electronically sent from one location to one or more other locations.

Transmission Control Protocol/Internet Protocol (TCP/IP) - This is the suite of protocols that defines the *Internet*. Originally designed for the *UNIX* operating system, TCP/IP software is now included with every major kind of computer operating system. To be truly on the *Internet*, your computer must have TCP/IP software.

Transmission Security – (TRANSEC) Measures (security controls) applied to transmissions in order to prevent interception, disruption of reception, communications deception, and/or derivation of intelligence by analysis of transmission characteristics such as signal parameters or message externals.
Note: TRANSEC is that field of COMSEC which deals with the security of communication transmissions, rather than that of the information being communicated.

Trap Door – A means of reading cryptographically protected information by the use of private knowledge of weaknesses in the cryptographic algorithm used to protect the data; in cryptography, one-to-one function that is easy to compute in one direction, yet believed to be difficult to invert without special information.

Transport Layer Security (TLS) – An authentication and security protocol widely implemented in browsers and Web servers.

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.

Trojan horse - A computer program is either hidden inside another program or that masquerades as something it is not in order to trick potential users into running it. For example a program that appears to be a game or image files but in reality performs some other function. The term "Trojan Horse" comes from a possibly mythical ruse of war used by the Greeks sometime between 1500 and 1200 B.C; a Trojan horse computer program may spread itself by sending copies of itself from the host computer to other computers, but unlike a *virus* it will (usually) not infect other programs; A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program.

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's 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. An established point of trust (usually based on the authority of some person, office, or organization) from which an entity begins the validation of an authorized process or authorized (signed) package. A "trust anchor" is sometimes defined as just a public key used for different purposes (e.g., validating a Certification Authority, validating a signed software package or key, validating the

process [or person] loading the signed software or key); A public or symmetric key that is trusted because it is directly built into hardware or software, or securely provisioned via out-of-band means, rather than because it is vouched for by another trusted entity (e.g. in a public key certificate).

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

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.

Trusted Certificate – Is 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."

Trusted Channel – A channel where the endpoints are known and data integrity is protected in transit. Depending on the communications protocol used, data privacy may be protected in transit. Examples include SSL, IPSEC, and secure physical connection.

Trusted Computer System – Is a system that employs sufficient hardware and software assurance measures to allow its use for processing simultaneously a range of sensitive or classified information.

Trusted Computing Base (TCB) – Totality of protection mechanisms within a computer system, including hardware, firmware, and software, the combination responsible for enforcing a security policy.

Trusted Distribution – Is the method for distributing trusted computing base (TCB) hardware, software, and firmware components that protects the TCB from modification during distribution.

Trusted Foundry – Facility that produces integrated circuits with a higher level of integrity assurance.

Trusted Identification Forwarding – Identification method used in information system networks whereby the sending host can verify an authorized user on its system is attempting a connection to another host. The sending host transmits the required user authentication information to the receiving host.

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.

Trusted Path – 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.

Trusted Platform Module (TPM) Chip – A tamper-resistant integrated circuit built into some computer motherboards that can perform cryptographic operations (including key generation) and protect small amounts of sensitive information, such as passwords and cryptographic keys.

Trusted Process – Is a process that has been tested and verified to operate only as intended.

Trusted Recovery – Ability to ensure recovery without compromise after a system failure.

Trusted Software – Is the software portion of a trusted computing base (TCB).

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

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. The attribute of a person or enterprise that provides confidence to others of the qualifications, capabilities, and reliability of that entity to perform specific tasks and fulfill assigned responsibilities. Is the security decision with respect to extended investigations to determine and confirm qualifications, and suitability to perform specific tasks and responsibilities.

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.

TSEC – Telecommunications Security.

TSEC Nomenclature – System for identifying the type and purpose of certain items of COMSEC material.

Tunneling - A technique to encapsulate one communication data stream inside of another, in order to extend the advantages of the latter to the former. Attackers will often tunnel a network protocol that would not be allowed to cross network boundaries inside of another that is allowed, defeating perimeter defense; Technology enabling one network to send its data via another network's connections. Tunneling works by encapsulating a network protocol within packets carried by the second network.

Two-factor Authentication (T-FA) - Existing authentication methodologies involve three basic "factors":

• Something the user knows (e.g., password, PIN);
• Something the user has (e.g., ATM card, smart card); and
• Something the user is (e.g., biometric characteristic, such as a fingerprint).

T-FA requires that a user present two of the three possible factors to the Authentication mechanism. A known flaw in some T-FA systems is the server storage of a hash representation of the credentials contained on the smart card or token.

With this in hand, the attacker can replay that data to the authentication system; in this case, that of the proxy server, without needing the physical card or token.

Two-Part Code – Code consisting of an encoding section, in which the vocabulary items (with their associated code groups) are arranged in alphabetical or other systematic order, and a decoding section, in which the code groups (with their associated meanings) are arranged in a separate alphabetical or numeric order.

Two-Person Control (TPC) – Continuous surveillance and control of positive control material at all times by a minimum of two authorized individuals, each capable of detecting incorrect and unauthorized procedures with respect to the task being performed and each familiar with established security and safety requirements.

Two-Person Integrity (TPI) – System of storage and handling designed to prohibit individual access by requiring the presence of at least two authorized individuals, each capable of detecting incorrect or unauthorized security procedures with respect to the task being performed. See: No-Lone Zone.

Type Accreditation – Is a form of accreditation that is used to authorize multiple instances of a major application or general support system for operation at approved locations with the same type of computing environment. In situations where a major application or general support system is installed at multiple locations, a type accreditation will satisfy C&A requirements only if the application or system consists of a common set of tested and approved hardware, software, and firmware.

Type Certification – The certification acceptance of replica information systems based on the comprehensive evaluation of the technical and nontechnical security features of an information system and other safeguards, made as part of and in support of the formal approval process, to establish the extent to which a particular design and implementation meet a specified set of security requirements.

U

Unauthorized Access– Occurs when a user, legitimate or unauthorized, accesses a resource that the user is not permitted to use; any access that violates the stated security policy.

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

Unclassified – Information that has not been determined pursuant to E.O. 12958, as amended, or any predecessor order, to require protection against unauthorized disclosure and that is not designated as classified.

Uniform Resource Identifier (URI) - An address for resource available on the Internet. The first part of a URI is called the "scheme". The most well-known scheme is *http*, but there are many others. Each URI scheme has its own format for how a URI should appear. Here are examples of URIs using the *http*, *telnet*, and *news* schemes; In the Hypertext Transfer Protocol (HTTP), a string of characters that identifies an Internet

resource, including the type of resource and its location. There are two types of URIs: uniform resource locators (URLs) and relative URLs (RELURLs).

Uniform (Universal) Resource Locator (URL) – Is a way of specifying the location of publicly available information on the Internet; Also known as a Web address; the term URL is basically synonymous with *URI*. URI has replaced URL in technical specifications.

Uniform Resource Name (URN) - A *URI* that is supposed to be available for a long time. For an address to be a URN some institution is supposed to make a commitment to keep the resource available at that address.

UNIX – Is a computer operating system (the basic software running on a computer, underneath things like word processors and spreadsheets). UNIX is designed to be used by many people at the same time (it is multi-user) and has *TCP/IP* built-in. It is the most common operating system for *servers* on the *Internet*. Apple computers' Macintosh operating system, as of version 10 ("Mac OS X"), is based on Unix.

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

Untrusted Process – Process that has not been evaluated or examined for correctness and adherence to the security policy. It may include incorrect or malicious code that attempts to circumvent the security mechanisms.

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.

Update (key) – Automatic or manual cryptographic process that irreversibly modifies the state of a COMSEC key.

Upload - Transferring data (usually a file) from a computer you are using to another computer; the opposite of *download*.

USENET - A world-wide system of discussion groups, with comments passed among hundreds of thousands of machines. Not all USENET machines are on the *Internet*. USENET is completely decentralized, with over 10,000 discussion areas, called *newsgroups*.

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

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

User Datagram Protocol (UDP) - one of the protocols for data transfer that is part of the *TCP/IP* suite of protocols. UDP is a "stateless" protocol in that UDP makes no provision for acknowledgement of packets received.

User ID – Unique symbol or character string used by an information system to identify a specific user.

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

User Registration – Is a function in the life cycle of keying material; a process whereby an entity becomes a member of a security domain.

User Representative (COMSEC) – Individual authorized by an organization to order COMSEC keying material and interface with the keying system, provide information to key users, and ensure the correct type of key is ordered.

User Representative (Risk Management) – The person that defines the system's operational and functional requirements, and who is responsible for ensuring that user operational interests are met throughout the systems authorization process.

UUENCODE -- (UNIX to Unix Encoding) - A method for converting files from *Binary* to *ASCII* (text) so that they can be sent across the Internet via *email*.

V

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

Validation – The process of demonstrating that the system under consideration meets in all respects the specification of that system Confirmation (through the provision of strong, sound, objective evidence) that requirements for a specific intended use or application have been fulfilled (e.g., a trustworthy credential has been presented, or data or information has been formatted in accordance with a defined set of rules, or a specific process has demonstrated that an entity under consideration meets, in all respects, its defined attributes or requirements).

Variant – One of two or more code symbols having the same plain text equivalent.

Verification – Confirmation, through the provision of objective evidence, that specified requirements have been fulfilled (e.g., an entity's requirements have been correctly defined, or an entity's attributes have been correctly presented; or a procedure or function performs as intended and leads to the expected outcome).

Verified Name – Is a Subscriber name that has been verified by identity proofing.

Verifier – An entity that verifies the Claimant's identity by verifying the Claimant's possession and control 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.

Verifier – An entity which is or represents the entity requiring an authenticated identity. A verifier includes the functions necessary for engaging in authentication exchanges.

Verifier Impersonation Attack – Is a scenario where the Attacker impersonates the Verifier in an authentication protocol, usually to capture information that can be used to masquerade as a Claimant to the real Verifier.

Virtual Machine (VM) – Software that allows a single host to run one or more guest operating systems.

Virtual Private Network (VPN) – A virtual network, built on top of existing physical networks that provide a secure communications tunnel for data and other information transmitted between networks. Protected information system link utilizing tunneling, security controls (see Information Assurance), and endpoint address translation giving the impression of a dedicated line; Usually refers to a *network* in which some of the parts are connected using the public *Internet*, but the data sent across the Internet is encrypted, so the entire network is "virtually" private.

Virtual reality - Virtual reality is a computer simulation of a real three-dimensional world, often supplemented by sound effects. Examples include 3D flight simulators or first-person games where you explore 3D 'worlds'.

Virus – A computer program that can copy itself and infect a computer without permission or knowledge of the user. A virus might corrupt or delete data on a computer, use email programs to spread itself to other computers, or even erase everything on a hard disk.

Virus - A chunk of computer programming code that makes copies of itself without any conscious human intervention. Some viruses do more than simply replicate themselves, they might display messages, install other software or files, delete software of files, etc. A virus requires the presence of some other program to replicate itself. Typically viruses spread by attaching themselves to programs and in some cases files, for example the file formats for Microsoft word processor and spreadsheet programs allow the inclusion of programs called "macros" which can in some cases be a breeding ground for viruses.

Virus - A virus is a computer program that is designed to cause undesirable effects on computer systems. Viruses are often disguised as something else so that they can be transferred from one computer to another without the users knowing. They can be hidden in emails, on CDs or in files that are shared across the internet. Computer viruses can cause harm to computer systems and need to be avoided

Voice Over Internet Protocol (VOIP) - A specification and various technologies used to allow making telephone calls over *IP* networks, especially the *Internet*. Just as *modems* allow computers to connect to the Internet over regular telephone lines, VOIP technology allows humans to talk over Internet connections. Costs for VOIP calls can be a lot lower than for traditional telephone calls. Because the IP networks are *packet-switched* this allows for vastly different ways of handling connections and more efficient use of network resources; a technology that allows voice communication to be transmitted via the internet in the same way one might use a telephone to make a phone call. Popular use of VOIP technology is through the software Skype, which allows users to make video and phone calls via the internet for a relatively low cost to anywhere in the world.

Vulnerability – Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. Is a weakness in a system, application, or network that is subject to exploitation or misuse.

Vulnerability Analysis – See: Vulnerability Assessment.

Vulnerability Assessment – Formal description and evaluation of the vulnerabilities in an information system. Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

W

Walled Garden – Is an environment that controls the user's access to Web content and services. In effect, the walled garden directs the user's navigation within a website (blog), to allow access to a selection of material, or prevent access to other material.

Warm Site – An environmentally conditioned workspace that is partially equipped with information systems and telecommunications equipment to support relocated operations in the event of a significant disruption; backup site which typically contains the data links and preconfigured equipment necessary to rapidly start operations, but does not contain live data. Thus commencing operations at a warm site will (at a minimum) require the restoration of current data.

Web - Short for: "World Wide Web."

Web 1.0 – Websites that allow users to consume information. The information flow is one way in that users cannot produce information on a Web 1.0 site.

Web 2.0 (Read/Write Web) – Are websites that allow users to produce as well as consume information i.e. Blogs and wikis.

Web-based Distributed Authoring and Versioning (WebDAV)- A set of extensions to the *HTTP* protocol that allows multiple users to not only read but also to add, delete, and change documents residing on a web server. In order to use WebDAV you need WebDAV *client* software to connect to a HTTP *server* that has the WebDAV extensions installed. Virtually all common HTTP servers have WebDAV extensions available to them.

Web Bug – A tiny image, invisible to a user, placed on Web pages in such a way to enable 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 cookies. Malicious code, invisible to a user, placed on Web sites in such a way that it allows 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.

Web Content Filtering Software – A program that prevents access to undesirable Web sites, typically by comparing a requested Web site address to a list of known bad Web sites.

Web page - A document designed for viewing in a *web browser*; typically written in *HTML*. A *web site* is made of one or more web pages.

Web Risk Assessment – Processes for ensuring Web sites are in compliance with applicable policies.

Website- The entire collection of *web pages* and other information (such as images, sound, and video files, etc.) that are made available through what appears to users as a single web server.

Whaling - A digital con game meant to swindle corporate employees, especially those of upper position, into divulging confidential information on their databases. Unlike in phishing and pharming however, masqueraded web pages and electronic mails will take more serious executive-level form such as a written subpoena, customer complaint, or executive issue.

Whitelist – Is a list of discrete entities, such as hosts or applications that are known to be benign and are approved for use within an organization and/or information system.

White Team – Is the group responsible for refereeing an engagement between a Red Team of mock attackers and a Blue Team of actual defenders of their enterprise's use of information systems. In an exercise, the White Team acts as the judges, enforces the rules of the exercise, observes the exercise, scores teams, resolves any problems that may arise, handles all requests for information or questions, and ensures that the competition runs fairly and does not cause operational problems for the defender's mission. The White Team helps to establish the rules of engagement, the metrics for assessing results and the procedures for providing operational security for the engagement. The White Team normally has responsibility for deriving lessons-learned, conducting the post engagement assessment, and promulgating results; Can also refer to a small group of people who have prior knowledge of unannounced Red Team activities. The White Team acts as observers during the Red Team activity and ensures the scope of testing does not exceed a predefined threshold.

Wide Area Information Servers (WAIS) - Developed in the early 1990s WAIS was the first truly large-scale system to allow the indexing of huge quantities of information on the *Web*, and to make those indices searchable across *networks* such as the *Internet*. WAIS was also pioneering in its use of ranked (scored) results where the software tries to determine how relevant each result it.

Wide Area Network (WAN) - Any *internet* or *network* that covers an area larger than a single building or campus.

Wiki - A wiki is a web site for which the content can be easily edited and altered from the web browser in which you are viewing it. Typically there is an "edit" button on each page and the wiki is configured to allow either anyone or only people with

passwords to edit each page. The word "wiki" comes from a Hawaiian word meaning "quick"; Web applications or similar tools that allow identifiable users to add content (as in an Internet forum) and allow anyone to edit that content collectively.

Wired Equivalent Privacy (WEP) – A security protocol, specified in the IEEE 802.11 standard, that is designed to provide a WLAN with a level of security and privacy comparable to what is usually expected of a wired LAN. WEP is no longer considered a viable encryption mechanism due to known weaknesses.

Wireless Access Point (WAP) – A device that acts as a conduit to connect wireless communication devices together to allow them to communicate and create a wireless network.

Wireless Application Protocol (WAP) – A standard that defines the way in which Internet communications and other advanced services are provided on wireless mobile devices.

Wireless Fidelity (Wi-Fi) - A popular term for a form of wireless data communication, basically Wi-Fi is "Wireless Ethernet".

Wireless Fidelity (Wi-Fi) internet access - Wi-Fi (wireless) internet access is wireless networking technology that uses radio waves to provide wireless high-speed internet and network connections. Wi-Fi works with no physical wired connection between sender and receiver by using radio frequency technology. In order to connect to an access point and join a wireless network, computers and devices must be equipped with wireless network adapters.

Wireless Fidelity Protected Access-2 (WPA2) – Is the approved Wi-Fi Alliance interoperable implementation of the IEEE 802.11i security standard.

Wireless Local Area Network (WLAN) – A group of wireless networking devices within a limited geographic area, such as an office building, that exchange data through radio communications. The security of each WLAN is heavily dependent on how well each WLAN component—including client devices, APs, and wireless switches—is secured throughout the WLAN lifecycle, from initial WLAN design and deployment through ongoing maintenance and monitoring.

Wireless Technology – Technology that permits the transfer of information between separated points without physical connection.
Note: Currently wireless technologies use infrared, acoustic, radio frequency, and optical.

Work craft Identity – Synonymous with: Tradecraft Identity.

Work Factor – Estimate of the effort or time needed by a potential perpetrator, with specified expertise and resources, to overcome a protective measure.

World Wide Web - The World wide web or 'web' as it is more commonly called, is a collection of pages on the internet that can be read accessed with any web enable devise such as mobile phone, PDA and computers. Users need an internet connection, a computer, a web browser, in order to access and interact with the online information that forms part of the web.

Worm – A self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself. See Malicious Code; A worm is a *virus* that does not infect other programs. It makes copies of itself, and infects additional computers (typically by making use of network connections) but does not attach itself to additional programs; however a worm might alter, install, or destroy files and programs.

Write – Fundamental operation in an information system that results only in the flow of information from a subject to an object. See Access Type.

Write Access – Permission to write to an object in an information system.

Write-Blocker – A device that allows investigators to examine media while

World Wide Web (WWW)- World Wide Web (or simply Web for short) is a term frequently used (incorrectly) when referring to "The Internet", WWW has two major meanings: First, loosely used: the whole constellation of resources that can be accessed using *Gopher, FTP, HTTP,telnet, USENET, WAIS* and some other tools; Second, the universe of hypertext *servers (HTTP servers)*, more commonly called "web servers", which are the servers that serve *web pages* to web *browsers*.

X

X.509 Certificate – The X.509 public-key certificate or the X.509 attribute certificate, as defined by the ISO/ITU-T X.509 standard. Most commonly (including in this document), an X.509 certificate refers to the X.509 public-key certificate.

X.509 Public Key Certificate – A digital certificate containing a public key for entity and a name for the entity, together with some other information that is 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.

XHTML (eXtensible HyperText Markup Language) – Basically *HTML* expressed as valid *XML*. XHTML is intended to be used in the same places you would use HTML (creating web pages) but is much more strictly defined, which makes it a lot easier to create sofware that can read it, edit it, check it for errors, etc. XHTML is expected to eventually replace HTML.

XML (eXtensible Markup Language) – A widely used system for defining data formats. XML provides a very rich system to define complex documents and data structures such as invoices, molecular data, news feeds, glossaries, inventory descriptions, real estate properties, etc; As long as a programmer has the XML definition for a collection of data (often called a "schema") then they can create a

program to reliably process any data formatted according to those rules. XML is a subset of the older *SGML* specification - the definition of XML is SGML minus a couple of dozen items.

XMLRPC (XML Remote Procedure Call) – Is a *protocol* for *client-server* communication that sends and receives information "on top of" *HTTP*. The data sent and received is in a particular *XML*format specifically designed for use with XMLRPC.

XPFE (Cross Platform Front End) – A suite of technologies used to create applications that will work and look the same on different computer operating systems. A widely used XPFE application is the Mozilla web browser and its derivities, such as the Netscape web browser in version 7 and later. The primary technologies used in creating XPFE applications are *JavaScript*, *Cascading Style Sheets*, and *XUL*.

XUL (eXtensible User-interface Language) – A markup language similar to *HTML* and based on *XML*. XUL used to define what the user interface will look like for a particular piece of software. XUL is used to define what buttons, scrollbars, text boxes, and other user-interface items will appear, but it is not used to define how those items will look (e.g. what color they are). The most widely used example of XUL use is probably in the Firefox web browser, where the entire users interface is defined using the XUL language.

Z

Zero day exploit – An attack against a software vulnerability that has not yet been addressed by the software maintainers. These attacks are difficult to defend against as they are often undisclosed by the vendor until a fix is available, leaving victims unaware of the exposure.

Zero Fill – adapted to fill unused storage locations in an information system with the representation of the character denoting "0."

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. A method of erasing electronically stored data, cryptographic keys, and Credentials Service Providers (CSPs) by altering or deleting the contents of the data storage to prevent recovery of the data.

Zeroize – To remove or eliminate the key from a cryptographic equipment or fill device. Overwrite a memory location with data consisting entirely of bits with the value zero so that the data is destroyed and not recoverable. This is often contrasted with deletion methods that merely destroy reference to data within a file system rather than the data itself.

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

Zone Of Control – Three-dimensional space surrounding equipment that processes classified and/or sensitive information within which TEMPEST exploitation is not considered practical or where legal authority to identify and remove a potential TEMPEST exploitation exists.

REFERENCES:

Commonwealth Fusion Center. Commonwealth Critical Infrastructure Program. Glossary of Cyber Security Terms. Massachusetts, U.S.A.: Commonwealth Fusion Center, April 2012. Web. 08 November 2013 <http://www.nedrix.com/downloads/U_Glossary%20of%20Cyber%20Security%20Terms.pdf>.

Commonwealth of Australia. "Glossary." *Cyber(smart:)*. Commonwealth of Australia, 2013. Web. 08 November 2013 <http://www.cybersmart.gov.au/glossary.aspx>.

Elk Grove Unified School District (EGUSD). *Cyberspace Glossary.* Web. 08 November 2013 <http://www.egusd.net/students_parents/pdfs/CyberspaceGlossary2.pdf >.

Enzer, Matisse. *Glossary of Internet Terms*. Matisse Enzer, 2011. Web. 08 November 2013 < http://www.matisse.net/files/glossary.html>.

LexisNexis. "Cyberspace Glossary." *LexisNexis Legal Newsroom*. LexisNexis, 2013. Web. 08 November 2013 < http://www.lexisnexis.com/legalnewsroom/lexis-hub/b/legal-technology-and-social-media/archive/2008/12/16/cyberspace glossary.aspx>.

PCTools. "Security News." *PCTools by Symantec*. PCTools, 2010. Web. 08 November 2013 <http://www.pctools.com/security-news/definitionof-a-hacker/>.

United States. Committee on National Security Systems (CNSS). *National Information Assurance (IA) Glossary*. Maryland, U.S.A.: CNSS, April 2010. Web. 08 November 2013 < http://www.ncix.gov/publications/policy/docs/CNSSI_4009.pdf>.

United States. Department of Commerce. National Institute of Standards and Technology. *Glossary of Key Information Security Terms*. Maryland: NIST, May 2013. Web. 08 November 2013 <http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf>.

United States. Department of Defense. The Vice Chairman of the Joint Chiefs of Staff. *Joint Terminology for Cyberspace Operations*. Washington, D.C. :DOD Web. 08 November 2013 <http://www.nsciva.org/CyberReferenceLib/2010 11-Joint%20Terminology%20for%20Cyberspace%20Operations.pdf>.

United States. Department of Homeland Security. National Initiative for Cybersecurity Careers and Studies (NICCS). *Explore Terms: A Glossary of Common Cybersecurity Terminology.* DHS-NICCS. Web. 08 November 2013 <http://niccs.us-cert.gov/glossary>.

University of Texas at Austin. "Cybersecurity Glossary Terms." *Information Technology Services.* Information Technology Services, 2013. Web. 08 November 2013 <http://www.utexas.edu/its/glossary/secure>.