CISSP GLOSSARY

TSV 413: CISSP CBK Review Course

Version 1.1

April 2, 2010

CONTENTS

[SECTION I: TERMS AND DEFINITIONS 3](#_Toc217549946)

[A 3](#_Toc217549947)

[B 6](#_Toc217549948)

[C 7](#_Toc217549949)

[D 18](#_Toc217549950)

[E 21](#_Toc217549951)

[F 23](#_Toc217549952)

[G 25](#_Toc217549953)

[H 25](#_Toc217549954)

[I 26](#_Toc217549955)

[K 30](#_Toc217549956)

[L 31](#_Toc217549957)

[M 32](#_Toc217549958)

[N 35](#_Toc217549959)

[O 36](#_Toc217549960)

[P 38](#_Toc217549961)

[Q 41](#_Toc217549962)

[R 41](#_Toc217549963)

[S 43](#_Toc217549964)

[T 49](#_Toc217549965)

[U 53](#_Toc217549966)

[V 55](#_Toc217549967)

[W 55](#_Toc217549968)

[Z 56](#_Toc217549969)

[SECTION II: COMMONLY USED ABBREVIATIONS AND ACRONYMS 57](#_Toc217549970)

[SECTION III: REFERENCES 70](#_Toc217549971)

# SECTION I: TERMS AND DEFINITIONS

## A

|  |  |
| --- | --- |
| Access | Opportunity to make use of an information system (IS) resource. |
| Access control | Limiting access to information system resources only to authorized users, programs, processes, or other systems. |
| Access control list (ACL) | Mechanism implementing discretionary and/or mandatory access control between subjects and objects. |
| Access control mechanism | Security safeguard designed to detect and deny unauthorized access and permit authorized access in an information system. |
| Access level | Hierarchical portion of the security level used to identify the sensitivity of information system data and the clearance or authorization of users. Access level, in conjunction with the nonhierarchical categories, forms the sensitivity label of an object. (See category.) |
| Access list | (IS) Compilation of users, programs, or processes and the access levels and types to which each is authorized.  (COMSEC) Roster of individuals authorized admittance to a controlled area. |
| Access profile | Associates each user with a list of protected objects the user may access. |
| Access type | Privilege to perform action on an object. Read, write, execute, append, modify, delete, and create are examples of access types. (See write.) |
| Accountability | (IS) Process of tracing information system activities to a responsible source.  (COMSEC) 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. |
| Accreditation | Formal declaration by a Designated Accrediting Authority (DAA) 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. (See security safeguards.) |
| Accrediting authority | Synonymous with Designated Accrediting Authority (DAA). |
| Adequate security | Security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information. This includes assuring that information systems operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost-effective management, personnel, operational, and technical controls. (OMB Circular A-130) |
| Advanced Encryption Standard (AES) | FIPS approved cryptographic algorithm that is a symmetric block cipher using cryptographic key sizes of 128, 192, and 256 bits to encrypt and decrypt data in blocks of 128 bits. |
| Advisory | Notification of significant new trends or developments regarding the threat to the information system of an organization. This notification may include analytical insights into trends, intentions, technologies, or tactics of an adversary targeting information systems. |
| Alert | Notification that a specific attack has been directed at the information system of an organization. |
| 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. |
| Assurance | Measure of confidence that the security features, practices, procedures, and architecture of an information system accurately mediates and enforces the security policy. |
| Attack | Attempt to gain unauthorized access to an information system’s services, resources, or information, or the attempt to compromise an information system’s integrity, availability, or confidentiality. |
| Audit | Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures. |
| Audit trail | Chronological record of system activities to enable the reconstruction and examination of the sequence of events and/or changes in an event. |
| Authenticate | To verify the identity of a user, user device, or other entity, or the integrity of data stored, transmitted, or otherwise exposed to unauthorized modification in an information system, or to establish the validity of a transmission. |
| Authentication | Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information. |
| Authentication system | Cryptosystem or process used for authentication. |
| Authenticator | Means used to confirm the identity of a station, originator, or individual. |
| Authorization | Access privileges granted to a user, program, or process. |
| Authorized vendor | Manufacturer of INFOSEC equipment authorized to produce quantities in excess of contractual requirements for direct sale to eligible buyers. Eligible buyers are typically U.S. Government organizations or U.S. Government contractors. |
| Authorized Vendor Program (AVP) | Program in which a vendor, producing an INFOSEC product under contract to NSA, is authorized to produce that product in numbers exceeding the contracted requirements for direct marketing and sale to eligible buyers. Eligible buyers are typically U.S. Government organizations or U.S. Government contractors. Products approved for marketing and sale through the AVP are placed on the Endorsed Cryptographic Products List (ECPL). |
| Availability | “Ensuring timely and reliable access and use of information.” (44 USC Sec. 3542) |

## B

|  |  |
| --- | --- |
| Back door | Hidden software or hardware mechanism used to circumvent security controls. Synonymous with trap door. |
| Backup | Copy of files and programs made to facilitate recovery, if necessary. |
| Banner | Display on an information system that sets parameters for system or data use. |
| Bell-LaPadula | A formal state transition model of computer security policy that describes a set of access control rules that uses security labels on objects and clearances for subjects. It was developed by David E. Bell and Leonard J. LaPadula. Bell-LaPadula security model is for meeting the confidentiality security objective only. |
| Benign | Condition of cryptographic data that cannot be compromised by human access. |
| Benign environment | Non-hostile environment that may be protected from external hostile elements by physical, personnel, and procedural security countermeasures. |
| Biba | A formal state transition access control security model that focuses on data integrity in an information system. In general, Biba integrity model has three goals: Prevent data modification by unauthorized subject, prevent unauthorized data modification by authorized subject, and maintain internal and external consistency. It is defined by Kenneth J. Biba. (A MITRE alumni) |
| Binding | Process of associating a specific communications terminal with a specific cryptographic key or associating two related elements of information. |
| biometrics | Automated methods of authenticating or verifying an individual based upon a physical or behavioral characteristic. |
| Bit error rate | Ratio between the number of bits incorrectly received and the total number of bits transmitted in a telecommunications system. |
| BLACK | Designation applied to information systems, and to associated areas, circuits, components, and equipment, in which national security information is encrypted or is not processed. |
| Boundary | Software, hardware, or physical barrier that limits access to a system or part of a system. |
| Browsing | Act of searching through information system storage to locate or acquire information, without necessarily knowing the existence or format of information being sought. |
| Bulk encryption | Simultaneous encryption of all channels of a multichannel telecommunications link. |

## C

|  |  |
| --- | --- |
| Call back | Procedure for identifying and authenticating a remote information system terminal, whereby the host system disconnects the terminal and reestablishes contact. Synonymous with dial back. |
| Central office | The physical building used to house inside plant equipment including telephone switches, which make telephone calls “work” in the sense of making connections and relaying the speech information. |
| Certificate | Digitally signed document that binds a public key with an identity. The certificate contains, at a minimum, the identity of the issuing Certification Authority, the user identification information, and the user’s public key. |
| Certificate management | Process whereby certificates (as defined above) are generated, stored, protected, transferred, loaded, used, and destroyed. |
| Certificate revocation list (CRL) | List of invalid certificates (as defined above) that have been revoked by the issuer. |
| Certification | Comprehensive evaluation of the technical and nontechnical 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 authority (CA) | (C&A) 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.  (PKI) Trusted entity authorized to create, sign, and issue public key certificates. By digitally signing each certificate issued, the user’s identity is certified, and the association of the certified identity with a public key is validated. | |
| Certification package | Product of the certification effort documenting the detailed results of the certification activities. | |
| Certification test and evaluation (CT&E) | 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 (NSTISSC)-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. | |
| Challenge and reply authentication | Prearranged procedure in which a subject requests authentication of another and the latter establishes validity with a correct reply. | |
| Checksum | Value computed on data to detect error or manipulation during transmission. (See hash total.) | |
| Check word | Cipher text generated by cryptographic logic to detect failures in cryptography. | |
| 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 | Enciphered information. | |
| Clark-Wilson | A formal security model to preserve information integrity in an information system. The model focuses on “well-formed” transaction using a set of enforcement and certification rules. It is developed by David D. Clark and David R. Wilson. | |
| Classified information | Information that has been determined pursuant to Executive Order 12958 or any predecessor Order, or by the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure and is marked to indicate its classified status. | |
| Classified information spillage | 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. | |
| Clearance | Formal security determination by an authorized adjudicative office that an individual is authorized access, on a need to know basis, to a specific level of collateral classified information (TOP SECRET, SECRET, CONFIDENTIAL). | |
| Client | 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 | 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. | |
| Confidentiality | “Preserving authorized restriction on information access and disclosure, including means for protecting personal privacy and proprietary information.” (44 USC Sec. 3542) | |
| Cold site | An inexpensive type of backup site with no IT infrastructure (e.g., computing and network hardware) in place. | |
| Cold start | Procedure for initially keying crypto-equipment. | |
| Collaborative computing | Applications and technology (e.g. , whiteboarding, group conferencing) that allow two or more individuals to share information real time in an inter- or intra-enterprise environment. | |
| Commercial COMSEC Evaluation Program (CCEP) | Relationship between NSA and industry in which NSA provides the COMSEC expertise (i.e., standards, algorithms, evaluations, and guidance) and industry provides design, development, and production capabilities to produce a type 1 or type 2 product. Products developed under the CCEP may include modules, subsystems, equipment, systems, and ancillary devices. | |
| Common Criteria | Provides a comprehensive, rigorous method for specifying security function and assurance requirements for products and systems. (International Standard ISO/IEC 5408, Common Criteria for Information Technology Security Evaluation [ITSEC]) | |
| Communications deception | Deliberate transmission, retransmission, or alteration of communications to mislead an adversary’s interpretation of the communications. (See imitative communications deception and manipulative communications deception.) | |
| 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) | (COMSEC) Measures and controls taken to deny unauthorized individuals information derived from telecommunications and to ensure the authenticity of such telecommunications. Communications security includes cryptosecurity, transmission security, emission security, and physical security of COMSEC material. | |
| 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: (a) valid security clearance for the most restricted information processed in the system; (b) formal access approval and signed nondisclosure agreements for that information which a user is to have access; and (c) valid need-to-know for information which a user is to have access. | |
| Compromise | Type of incident where information is disclosed to unauthorized individuals 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 systems equipment. (See TEMPEST.) | |
| Computer abuse | Intentional or reckless misuse, alteration, disruption, or destruction of information processing resources. | |
| Computer cryptography | Use of a crypto-algorithm program by a computer to authenticate or encrypt/decrypt information. | |
| Computer security | 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 incident | See incident. | |
| Computer security subsystem | Hardware/software designed to provide computer security features in a larger system environment. Computing environment 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 assembly | Group of parts, elements, subassemblies, or circuits that are removable items of COMSEC equipment. | |
| 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 element | Removable item of COMSEC equipment, assembly, or subassembly; normally consisting of a single piece or group of replaceable parts. | |
| 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 crypto-equipment, crypto-ancillary equipment, crypto-production equipment, and authentication equipment. | |
| COMSEC facility | Authorized and approved space used for generating, storing, repairing, or using COMSEC material. | |
| COMSEC incident | See incident. | |
| COMSEC manager | 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 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 training | Teaching of skills relating to COMSEC accounting, use of COMSEC aids, or installation, use, maintenance, and repair of COMSEC equipment. | |
| Concept of operations (CONOP) | Document detailing the method, act, process, or effect of using an information system. | |
| Confidentiality | Assurance that information is not disclosed to unauthorized individuals, processes, or devices. | |
| Configuration control | Process of controlling modifications to hardware, firmware, software, and documentation to ensure the information system is protected against improper modifications prior to, during, and after system implementation. | |
| Configuration management | Management of security features and assurances through control of changes made to hardware, software, firmware, documentation, test, test fixtures, and test documentation throughout the life cycle 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.) | |
| Continuity of operations plan | Plan for continuing an organization’s (usually a (COOP) headquarters element) essential functions at an alternate site and performing those functions for the duration of an event with little or no loss of continuity before returning to normal operations. | |
| 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 | 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 cryptographic item (CCI) | Secure telecommunications or information handling equipment, or associated cryptographic component, that is unclassified but governed by a special set of control requirements. Such items are marked “CONTROLLED CRYPTOGRAPHIC ITEM” or, where space is limited, “CCI.” | |
| Controlled interface | Mechanism that facilitates the adjudication of different interconnected system security policies (e.g., controlling the flow of information into or out of an interconnected system). | |
| 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. | |
| Countermeasure | Action, device, procedure, technique, or other measure that reduces the vulnerability of an information system. | |
| Covert channel | Unintended and/or unauthorized communications path that can be used to transfer information in a manner that violates an information system security policy. (See overt channel and exploitable 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 | 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 | 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. | |
| Credentials | Information, passed from one entity to another, used to establish the sending entity’s access rights. | |
| Critical infrastructures | System and assets, whether physical or virtual, so vital to the U.S. that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. [Critical Infrastructures Protection Act of 2001, 42 U.S.C. 5195c(e)] | |
| Cross domain solution | Information assurance solution that provides the ability to access or transfer information between two or more security domains. (See multi level security.) | |
| Cryptanalysis | Operations performed in converting encrypted messages to plain text without initial knowledge of the crypto-algorithm and/or key employed in the encryption. | |
| CRYPTO | Marking or designator identifying COMSEC keying material used to secure or authenticate telecommunications carrying classified or sensitive U.S. Government or U.S. Government-derived information. | |
| Crypto-alarm | Circuit or device that detects failures or aberrations in the logic or operation of crypto-equipment. Crypto-alarm may inhibit transmission or may provide a visible and/or audible alarm. | |
| Crypto-algorithm | Well-defined procedure or sequence of rules or steps, or a series of mathematical equations used to describe cryptographic processes such as encryption/decryption, key generation, authentication, signatures, etc. | |
| Crypto-ancillary equipment | Equipment designed specifically to facilitate efficient or reliable operation of crypto-equipment, without performing cryptographic functions itself. | |
| Crypto-equipment | Equipment that embodies a cryptographic logic. | |
| Cryptographic | Pertaining to, or concerned with, cryptography. | |
| Cryptographic component | 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 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) cryptoalgorithm(s) along with alarms, checks, and other processes essential to effective and secure performance of the cryptographic process(es). | |
| Cryptographic randomization | Function that randomly determines the transmit state of a cryptographic logic. | |
| Cryptography | Art or science concerning the principles, means, and methods for rendering plain information unintelligible and for restoring encrypted information to intelligible form. | |
| Crypto-ignition key (CIK) | Device or electronic key used to unlock the secure mode of crypto-equipment. | |
| Cryptology | Field encompassing both cryptography and cryptanalysis. | |
| Crypto-period | Time span during which each key setting remains in effect. | |
| Crypto-security | Component of COMSEC resulting from the provision of technically sound cryptosystems and their proper use. | |
| Crypto-synchronization | Process by which a receiving decrypting cryptographic logic attains the same internal state as the transmitting encrypting logic. | |
| Cryptosystem | Associated INFOSEC items interacting to provide a single means of encryption or decryption. | |
| Cryptosystem analysis | Process of establishing the exploitability of a cryptosystem, normally by reviewing transmitted traffic protected or secured by the system under study. | |
| Cryptosystem evaluation | Process of determining vulnerabilities of a cryptosystem. | |
| Cryptosystem review | Examination of a cryptosystem by the controlling authority ensuring its adequacy of design and content, continued need, and proper distribution. | |
| Cryptosystem survey | Management technique in which actual holders of a cryptosystem express opinions on the system’s suitability and provide usage information for technical evaluations. | |
| Cyclic redundancy check | Error checking mechanism that checks data integrity by computing a polynomial algorithm based checksum. | |

## D

|  |  |
| --- | --- |
| Data aggregation | Compilation of unclassified individual data systems and data elements that could result in the totality of the information being classified or of beneficial use to an adversary. |
| Data Encryption Standard (DES) | Cryptographic algorithm, designed for the protection of unclassified data and published by the National Institute of Standards and Technology (NIST) in Federal Information Processing Standard (FIPS) Publication 46. (FIPS 46-3 withdrawn 19 May 2005) (See Triple DES) and CNSS Advisory IA/02-04 Revised March 2005) |
| Data flow control | Synonymous with information flow control. |
| Data integrity | Condition existing when data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed. |
| Data origin authentication | Corroborating the source of data is as claimed. |
| Data security | Protection of data from unauthorized (accidental or intentional) modification, destruction, or disclosure. |
| 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. |
| 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. |
| Dedicated mode | information system 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: a. valid security clearance for all information within the 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 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 | Temporary 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-depth | IA strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and dimensions of networks. Synonymous with security-in-depth. |
| Degaussing | Procedure that reduces 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. |
| Denial of service | Any action or series of actions that prevents any part of an information system from functioning. |
| Descriptive top-level specification | Top-level specification written in a natural language (e.g., English), an informal design notation, or a combination of the two. Descriptive top-level specification, required for a class B2 and B3 (as defined in the Orange Book, Department of Defense Trusted Computer System Evaluation Criteria, DoD 5200.28-STD) information system, completely and accurately describes a trusted computing base. (See formal top-level specification.) |
| 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. |
| Dial back | Synonymous with call back. |
| Digital signature | Cryptographic process used to assure message originator authenticity, integrity, and non-repudiation. Synonymous with electronic signature. |
| Digital signature algorithm | Procedure that appends data to, or performs a cryptographic transformation of, a data unit. The appended data or cryptographic transformation allows reception of the data unit and protects against forgery, e.g., by the recipient. |
| Direct shipment | Shipment of COMSEC material directly from NSA to user COMSEC accounts. |
| Disaster recovery plan | Provides for the continuity of system operations after a disaster. |
| Discretionary access control (DAC) | Means of restricting access to objects based on the (DAC) identity and need-to-know of users and/or groups to which the object belongs. Controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (directly or indirectly) to any other subject. (See mandatory access control.) |
| Distinguished name | Globally unique identifier representing an individual’s identity. |
| DMZ (Demilitarized Zone) | Perimeter network segment that is logically between internal and external networks. Its purpose is to enforce the internal network’s IA policy for external information exchange and to provide external, un-trusted sources with restricted access to releasable information while shielding the internal networks from outside attacks. A DMZ is also called a “screened subnet.” |
| Domain | System or group of systems operating under a common security policy. |

## E

|  |  |
| --- | --- |
| 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. |
| 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 security (ELSEC) | Protection resulting from measures designed to deny unauthorized individuals information derived from the interception and analysis of noncommunications electromagnetic radiations. |
| Electronic signature | See digital signature. |
| Embedded computer | Computer system that is an integral part of a larger system. |
| Embedded cryptography | Cryptography engineered into an equipment or system whose basic function is not cryptographic. |
| Embedded cryptographic system | Cryptosystem performing or controlling a function as an integral element of a larger system or subsystem. |
| Emissions security (EMSEC) | Protection resulting from measures taken to deny unauthorized individuals information derived from intercept and analysis of compromising emanations from crypto-equipment or an information system. (See TEMPEST.) |
| Encipher | Convert plain text to cipher text by means of a cryptographic system. |
| Enclave | Collection of computing environments connected by one or more internal networks under the control of a single authority and security policy, including personnel and physical security. |
| 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 encipher and encode. |
| Encryption algorithm | Set of mathematically expressed rules for rendering data unintelligible by executing a series of conversions controlled by a key. |
| End-item accounting | Accounting for all the accountable components of a COMSEC equipment configuration by a single short title. |
| End-to-end encryption | Encryption of information at its origin and decryption at its intended destination without intermediate decryption. |
| End-to-end security | Safeguarding information in an information system from point of origin to point of destination. |
| Endorsed for unclassified cryptographic item (EUCI) | Unclassified cryptographic equipment that embodies a U.S. Government classified cryptographic logic and is endorsed by NSA for the protection of national security information. (See type 2 product.) |
| Endorsement | NSA approval of a commercially developed product for safeguarding national security information. |
| Entrapment | Deliberate planting of apparent flaws in an information system for the purpose of detecting attempted penetrations. |
| Environment | 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. |
| Evaluation Assurance Level (EAL) | Set of assurance requirements that represent a point on the Common Criteria predefined assurance scale. |
| Event | Occurrence, not yet assessed, that may affect the performance of an information system. |
| Executive state | One of several states in which an information system may operate, and the only one in which certain privileged instructions may be executed. Such privileged instructions cannot be executed when the system is operating in other states. Synonymous with supervisor state. |
| Exercise key | Key used exclusively to safeguard communications transmitted over-the-air during military or organized civil training exercises. |
| Exploitable channel | 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. (See covert channel.) |
| Exposure | An information security "exposure" is a system configuration issue or a mistake in software that allows access to information or capabilities that can be used by a hacker as a stepping-stone into a system or network. |
| Extraction resistance | Capability of crypto-equipment or secure telecommunications equipment to resist efforts to extract key. |
| Extranet | Extension to the intranet allowing selected outside users access to portions of an organization’s intranet. |

## F

|  |  |
| --- | --- |
| 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. |
| 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 limited to authorized users only. |
| Fill device | COMSEC item used to transfer or store key in electronic form or to insert key into a crypto-equipment. |
| FIREFLY | Key management protocol based on public key cryptography. |
| Firewall | System designed to defend against unauthorized access to or from a private network. |
| Firmware | Program recorded in permanent or semi-permanent computer memory. |
| Fixed COMSEC facility | COMSEC facility located in an immobile structure or aboard a ship. |
| Flaw | Error of commission, omission, or oversight in an information system that may allow protection mechanisms to be bypassed. |
| Flaw hypothesis methodology | 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 | Type of incident involving insertion of a large volume of data resulting in denial of service. |
| Formal access approval | Process for authorizing access to classified or sensitive information with specified access requirements, such as Sensitive Compartmented Information (SCI) or Privacy Data, based on the specified access requirements and a determination of the individual’s security eligibility and need-to-know. |
| Formal development | Software development strategy that proves security methodology design specifications. |
| Formal method | Mathematical argument which verifies that the system satisfies a mathematically described security policy. |
| Formal proof | Complete and convincing mathematical argument presenting the full logical justification for each proof step and for the truth of a theorem or set of theorems. |
| Formal security policy | Mathematically precise statement of a security policy. |
| Formal top-level specification | Top-level specification written in a formal mathematical language to allow theorems, showing the correspondence of the system specification to its formal requirements, to be hypothesized and formally proven. |
| Formal verification | Process of using formal proofs to demonstrate the consistency between formal specification of a system and formal security policy model (design verification) or between formal specification and its high-level program implementation (implementation verification). |
| Frequency hopping | Repeated switching of frequencies during radio transmission according to a specified algorithm, to minimize unauthorized interception or jamming of telecommunications. |
| Front-end security filter | Security filter logically separated from the remainder of an information system to protect system integrity. Synonymous with firewall. |
| Full maintenance | Complete diagnostic repair, modification, and overhaul of COMSEC equipment, including repair of defective assemblies by piece part replacement. (See limited maintenance.) |
| Functional proponent | See network sponsor. |
| Functional testing | Segment of security testing in which advertised security mechanisms of an information system are tested under operational conditions. |

## G

|  |  |
| --- | --- |
| Gateway | Interface providing a compatibility between networks by converting transmission speeds, protocols, codes, or security measures. |
| Global Information Grid | The globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to war fighters, policy makers, and support personnel. (DoD Directive 8100.1, 19 Sept. 2002) |
| Guard | Mechanism limiting the exchange of information between systems. |

## H

|  |  |
| --- | --- |
| Hacker | Unauthorized user who attempts to or gains access to an information system. |
| Handshaking procedures | Dialogue between two information system’s 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). |
| Hardwired key | Permanently installed key. |
| Hash total | Value computed on data to detect error or manipulation. (See checksum.) |
| Hashing | Computation of a hash total. |
| Hash word | Memory address containing hash total. |
| High assurance guard (HAG) | Device comprised of both hardware and software that is designed to enforce security rules during the transmission of X.400 message and X.500 directory traffic between enclaves of different classification levels (e.g., UNCLASSIFIED and SECRET). |
| Hot site | A backup site that is a duplicate of original data center with full IT computing infrastructure and replicated data. It is the most expensive business continuity solution. |

## I

|  |  |
| --- | --- |
| IA architecture | Activity that aggregates the functions of developing IA operational, system, and technical architecture products for the purpose of specifying and implementing new or modified IA capabilities within the IT environment. (DoD Directive 8100.1, 19 Sept 2002) |
| 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. |
| Identification | Process an information system uses to recognize an entity. |
| Identity token | Smart card, metal key, or other physical object used to authenticate identity. |
| Identity validation | Tests enabling an information system to authenticate users or resources. |
| Imitative communications deception | Introduction of deceptive messages or signals into an adversary’s telecommunications signals. (See communications deception and manipulative communications deception.) |
| Impersonating | Form of spoofing. |
| 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 | (IS) Assessed occurrence having actual or potentially adverse effects on an information system. (COMSEC) Occurrence that potentially jeopardizes the security of COMSEC material or the secure electrical transmission of national security information. |
| Incomplete parameter checking | 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. |
| Indicator | Recognized action, specific, generalized, or theoretical, that an adversary might be expected to take in preparation for an attack. |
| Individual accountability | Ability to associate positively the identity of a user with the time, method, and degree of access to an information system. |
| Informal security policy | Natural language description, possibly supplemented by mathematical arguments, demonstrating the correspondence of the functional specification to the high-level design. |
| 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 manager (IAM) | See information systems security manager. |
| Information assurance officer (IAO) | See information systems security officer. |
| Information assurance product | Product or technology 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. Examples include such products as data/network encryptors, firewalls, and intrusion detection devices. |
| Information environment | Aggregate of individuals, organizations, or systems that collect, process, or disseminate information, also included is the information itself. |
| Information flow control | Procedure to ensure that information transfers within an information system are not made from a higher security level object to an object of a lower security level. |
| Information operations (IO) | Actions taken to affect adversary information and information systems while defending one’s own information and information systems. |
| Information owner | Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal. |
| Information security policy | Aggregate of directives, regulations, rules, and practices that prescribe how an organization manages, protects, and distributes information. |
| Information system (IS) | Set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. |
| 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 engineering (ISSE) | Process that captures and refines information protection requirements and ensures their integration into IT acquisition processes 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 a program, organization, system, or enclave’s information assurance program. |
| Information systems security officer (ISSO) | Individual responsible to the ISSM for ensuring the appropriate operational IA posture is maintained for a system, program, or enclave. |
| Information systems security product | Item (chip, module, assembly, or equipment), technique, or service that performs or relates to information systems security. |
| Initialize | Setting the state of a cryptographic logic prior to key generation, encryption, or other operating mode. |
| Inspectable space | Three dimensional space surrounding equipment that process 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 | “Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.” (44 USC Sec. 3542) |
| Integrity check value | Checksum capable of detecting modification of an information system. |
| Interconnection security agreement | Written management authorization to interconnect information systems based upon acceptance of risk and implementation of established controls. |
| Interface | Common boundary between independent systems or modules where interactions take place. |
| Interface control document | Technical document describing interface controls and identifying the authorities and responsibilities for ensuring the operation of such controls. This document is baselined during the preliminary design review and is maintained throughout the information system lifecycle. |
| Interim Approval To Operate (IATO) | Temporary authorization granted by a DAA for an information system to process information based on preliminary results of a security evaluation of the system. |
| Interim Approval To Test (IATT) | 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 security controls | Hardware, firmware, or software features within an information system that restrict access to resources only to authorized subjects. |
| Internet Protocol (IP) | Standard protocol for transmission of data from source to destinations in packet-switched communications networks and interconnected systems of such networks. |
| IP broadcast methods | There are three methods:   * Unicast: Packet is sent from a single source to a single destination. * Broadcast: Source packet is copied and sent to all the nodes on a network. * Multicast: Source packet is copied and then sent to multiple destinations on a network. |
| Intrusion | Unauthorized act of bypassing the security mechanisms of a system. |

## K

|  |  |
| --- | --- |
| Key | Usually a sequence of random or pseudorandom bits used initially to set up and periodically change the operations performed in crypto-equipment for the purpose of encrypting or decrypting electronic signals, or for determining electronic counter countermeasures patterns, or for producing other key. |
| Key-auto-key (KAK) | Cryptographic logic using previous key to produce key. |
| Key distribution center (KDC) | COMSEC facility generating and distributing key in electrical form. |
| Key-encryption-key (KEK) | Key that encrypts or decrypts other key for transmission or storage. |
| Key exchange | Process of exchanging public keys (and other information) in order to establish secure communications. |
| Key list | Printed series of key settings for a specific cryptonet. Key lists may be produced in list, pad, or printed tape format. |
| Key management infrastructure (KMI) | Framework and services that provide the (KMI) generation, production, storage, protection, distribution, control, tracking, and destruction for all cryptographic key material, symmetric keys as well as public keys and public key certificates. |
| Key pair | Public key and its corresponding private key as used in public key cryptography. |
| Key production key (KPK) | Key used to initialize a keystream 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 updating | Irreversible cryptographic process for modifying key. |
| Keying material | Key, code, or authentication information in physical or magnetic form. |

## L

|  |  |
| --- | --- |
| label | See security label. |
| Labeled security protections | Elementary-level mandatory access control protection features and intermediate-level discretionary access control features in a TCB that uses sensitivity labels to make access control decisions. |
| Laboratory attack | Use of sophisticated signal recovery equipment in a laboratory environment to recover information from data storage media. |
| Least privilege | Principle requiring that each subject be granted the most restrictive set of privileges needed for the performance of authorized tasks. Application of this principle limits the damage that can result from accident, error, or unauthorized use of an information system. |
| 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 system and networks requiring implementation of standard minimum security countermeasures. 2. Medium: information system and networks requiring layering of additional safeguards above the standard minimum security countermeasures. 3. High: information system and networks requiring the most stringent protection and rigorous security countermeasures. |
| 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 | 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 authority | Organization responsible for generating and signing user certificates. |
| Local Management Device/ Key Processor (LMD/KP) | EKMS platform providing automated management of COMSEC material and generating key for designated users. Lock and key protection system Protection system that involves matching a key or password with a specific access requirement. Logic bomb Resident computer program triggering an unauthorized act when particular states of an information system are realized. |
| Logical completeness measure | Means for assessing the effectiveness and degree to which a set of security and access control mechanisms meets security specifications. |
| Long title | Descriptive title of a COMSEC item. |
| 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. |

## M

|  |  |
| --- | --- |
| 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. |
| Malicious applets | Small application programs automatically downloaded and executed 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. (See Trojan horse.) |
| malicious logic | Hardware, software, or firmware capable of performing an unauthorized function on an information system. |
| Mandatory access control (MAC) | Means of restricting access to objects based on the sensitivity 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. (See discretionary access control.) |
| mandatory modification | Change to a COMSEC end-item that NSA requires to be completed and reported by a specified date. (See optional modification.) |
| manipulative communications | Alteration or simulation of friendly deception 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 remote rekeying | Procedure by which a distant crypto-equipment is rekeyed electrically, with specific actions required by the receiving terminal operator. Synonymous with cooperative remote rekeying. (Also see automatic remote keying.) |
| masquerading | See spoofing. |
| Master crypto-ignition key | Key device with electronic logic and circuits providing the capability for adding more operational CIKs to a keyset. |
| Memory scavenging | The collection of residual information from data storage. |
| Message authentication code | Data associated with an authenticated message allowing a receiver to verify the integrity of the message. |
| 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 crypto-equipment. Some off-line cryptosystems, such as the KL-51 and one-time pad systems, employ message indicators to establish decryption starting points. |
| Mimicking | See spoofing. |
| Mobile code | Software modules obtained from remote systems, transferred across a network, and then downloaded and executed on local systems without explicit installation or execution by the recipient. |
| Mode of operation | 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. |
| Multilevel device | Equipment trusted to properly maintain and separate data of different security categories. |
| Multilevel mode | INFOSEC 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: a. some users do not have a valid security clearance for all the information processed in the information system; b. all users have the proper security clearance and appropriate formal access approval for that information to which they have access; and c. 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. (See cross domain solution.) |
| multi-security level (MSL) | Capability to process information of different security classifications or categories by using periods processing or peripheral sharing. |
| 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

|  |  |
| --- | --- |
| National Information Assurance Partnership (NIAP) | Joint initiative between NSA and NIST responsible for security testing needs of both IT consumers and producers and promoting the development of technically sound security requirements for IT products and systems and appropriate measures for evaluating those products and systems. |
| National Information Infrastructure (NII) | 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 information | Information that has been determined, pursuant to (NSI) Executive Order 12958 (as amended) (Ref b.) or any predecessor order, to require protection against unauthorized disclosure. |
| National security system | 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. (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). (Title 44 U.S. Code Section 3542, Federal Information Security Management Act of 2002.) |
| need-to-know | Necessity for access to, or knowledge or possession of, specific official information required to carry out official duties. |
| 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. |
| Network | information system implemented with a collection of interconnected nodes. |
| Network front-end | Device implementing protocols that allow attachment of a computer system to a network. |
| Network reference monitor | See reference monitor. |
| Network security | See information systems security. |
| Network security officer | See information systems security officer. |
| Network sponsor | 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 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. |
| No-lone zone | 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.) |
| Non-repudiation | Assurance the sender of data 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 data. |
| 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 | Passive entity containing or receiving information. Access to an object implies access to the information it contains. |
| Object reuse | Reassignment and re-use of a storage medium containing one or more objects after ensuring no residual data remains on the storage medium. |
| Official information | All information in the custody and control of a U.S. Government department or agency that was acquired by U.S. Government employees as a part of their official duties or because of their official status and has not been cleared for public release. |
| 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. |
| On-line cryptosystem | Cryptosystem in which encryption and decryption are performed in association with the transmitting and receiving functions. |
| Open storage | Storage of classified information within an accredited facility, but not in General Services Administration approved secure containers, while the facility is unoccupied by authorized personnel. |
| 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 that describes the presence of a 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. (See mandatory modification.) |
| Organizational maintenance | Limited maintenance performed by a user organization. |
| Organizational registration | Entity within the PKI that authenticates the authority (ORA) identity and the organizational affiliation of the users. |
| 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 crypto-equipment by sending new key directly to the remote crypto-equipment over the communications path it secures. |
| Overt channel | Communications path within a computer system or network designed for the authorized transfer of data. (See covert channel.) |
| Overwrite procedure | Process of writing patterns of data on top of the data stored on a magnetic medium. |

## P

|  |  |
| --- | --- |
| Parity | Bit(s) used to determine whether a block of data has been altered. |
| Partitioned security mode | information system 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. |
| Password | Protected/private string of letters, numbers, and special characters used to authenticate an identity or to authorize access to data. |
| Penetration | See intrusion. |
| Penetration testing | Security testing in which evaluators attempt to circumvent the security features of a system based on their understanding of the system design and implementation. |
| 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.) |
| Periods processing | 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. |
| Perimeter | 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. |
| Permuter | Device used in crypto-equipment to change the order in which the contents of a shift register are used in various nonlinear combining circuits. |
| Plain text | Unencrypted information. |
| Policy approving authority (PAA) | First level of the PKI Certification Management Authority that approves the security policy of each PCA. |
| Policy certification authority (PCA) | 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. |
| 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. |
| Pre-production 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. |
| Principal accrediting authority (PAA) | Senior official with authority and responsibility for all intelligence systems within an agency. |
| Print suppression | Eliminating the display of characters in order to preserve their secrecy. |
| Privacy system | Commercial encryption system that affords telecommunications limited protection to deter a casual listener, but cannot withstand a technically competent cryptanalytic attack. |
| Privileged user | Individual who has access to system control, monitoring, or administration functions (e.g., system administrator, system ISSO, maintainers, system programmers, etc.) |
| Probe | Type of incident involving an attempt to gather information about an information system for the apparent purpose of circumventing its security controls. |
| Production model | INFOSEC equipment in its final mechanical and electrical form. |
| Proprietary information | 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 systems (PDS) | Wire line or fiber optic distribution system used to transmit unencrypted classified national security information through an area of lesser classification or control. |
| 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. |
| Protection ring | One of a hierarchy of privileged modes of an information system that gives certain access rights to user programs and processes that are authorized to operate in a given mode. |
| 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. |
| Proxy | Software agent that performs a function or operation on behalf of another application or system while hiding the details involved. |
| 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 certificate | Contains the name of a user, the public key component of the user, and the name of the issuer who vouches that the public key component is bound to the named user. |
| Public key cryptography (PKC) | Encryption system using a linked pair of keys. What one key encrypts, the other key decrypts. |
| Public key infrastructure (PKI) | Framework established to issue, maintain, and revoke public key certificates accommodating a variety of security technologies, including the use of software. |
| Purging | Rendering stored information unrecoverable. (See sanitize.) |

## Q

|  |  |
| --- | --- |
| QUADRANT | Short name referring to technology that provides tamper-resistant protection to crypto-equipment. |

## R

|  |  |
| --- | --- |
| Randomizer | 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. |
| 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. |
| Real-time reaction | Immediate response to a penetration attempt that is detected and diagnosed in time to prevent access. |
| Recovery procedures | Actions necessary to restore data files of an information system and computational capability after a system failure. |
| RED | Designation applied to an information system, and associated areas, circuits, components, and equipment in which unencrypted national security information is being processed. |
| RED/BLACK concept | Separation of electrical and electronic circuits, components, equipment, and systems that handle national security information (RED), in electrical form, from those that handle non-national security information (BLACK) in the same form. |
| Red team | Interdisciplinary group of individuals authorized to conduct an independent and focused threat-based effort as a simulated adversary to expose and exploit system vulnerabilities for the purpose of improving the security posture of information systems. |
| RED signal | Any electronic emission (e.g., plain text, key, key stream, subkey stream, initial fill, or control signal) that would divulge national security information if recovered. |
| Reference Monitor | Concept of an abstract machine that enforces Target of Evaluation (TOE) access control policies. |
| 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. |
| Remanence | Residual information remaining on storage media after clearing. (See magnetic remanence and clearing.) |
| Remote access | Access for authorized users external to an enclave established through a controlled access point at the enclave boundary. |
| Remote rekeying | Procedure by which a distant crypto-equipment is rekeyed electrically. (See automatic remote rekeying and manual remote rekeying.) |
| 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. |
| Reserve keying material | Key held to satisfy unplanned needs. (See contingency key.) |
| Residual risk | 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. |
| Resource encapsulation | Method by which the reference monitor 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. |
| Risk | Possibility that a particular threat will adversely impact an information system by exploiting a particular vulnerability. |
| Risk analysis | Examination of information to identify the risk to an information system. |
| Risk assessment | Process of analyzing threats to and vulnerabilities of an information system, and the potential impact resulting from the loss of information or capabilities of a system. This analysis is used as a basis for identifying appropriate and cost-effective security countermeasures. |
| Risk index | Difference between the minimum clearance or authorization of information system users and the maximum sensitivity (e.g.; classification and categories) of data processed by the system. |
| Risk management | 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. (NIST Special Pub 800-53) |

## S

|  |  |
| --- | --- |
| Safeguard | 1. Protection included to counteract a known or expected condition.  2. Incorporated countermeasure or set of countermeasures within a base release. |
| 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. Synonymous with banner. |
| Sanitize | Process to remove information from media such that data recovery is not possible. It includes removing all classified labels, markings, and activity logs. (See purging.) |
| Scavenging | Searching through object residue to acquire data. |
| Secure communications | Telecommunications deriving security through use of type 1 products and/or PDSs. |
| Secure hash standard | Specification for a secure hash algorithm that can generate a condensed message representation called a message digest. |
| 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. |
| Security controls | 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. (NIST Special Pub 800-53) |
| Securety fault analysis | Assessment, usually performed on information system hardware, to (SFA) determine the security properties of a device when hardware fault is encountered. |
| Securety features users guide (SFUG) | Guide or manual explaining how the security mechanisms in a specific system work. |
| Security filter | information system trusted subsystem that enforces security policy on the data passing through it. |
| Security in depth | Synonymous with defense in depth. |
| 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 | Information representing the sensitivity of a subject or object, such as UNCLASSIFIED or its hierarchical classification (CONFIDENTIAL, SECRET, TOP SECRET) together with any applicable nonhierarchical security categories (e.g., sensitive compartmented information, critical nuclear weapon design information). |
| Security net control station | Management system overseeing and controlling implementation of network security policy. |
| Security perimeter | Boundary where security controls are in effect to protect assets. |
| Security range | Highest and lowest security levels that are permitted in or on an information system, system component, subsystem, or network. |
| Security requirements | Types and levels of protection necessary for equipment, data, information, applications, and facilities to meet information system security policy. |
| Security requirements baseline | Description of the minimum requirements necessary for an information system to maintain an acceptable level of security. |
| 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. (See accreditation.) |
| Security specification | Detailed description of the safeguards required to protect an information system. |
| Security target | 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 and 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. |
| 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 Central 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. |
| Sensitive information | Information, the loss, misuse, or unauthorized access to or modification of, that could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under 5 U.S.C. Section 552a (the Privacy Act), but that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy. (Systems that are not national security systems, but contain sensitive information, are to be protected in accordance with the requirements of the Computer Security Act of 1987 (P.L.100-235).) |
| 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. |
| Separation of duties | Concept of having more than one person required to complete a task. (Source: Wikipedia) |
| Shielded enclosure | Room or container designed to attenuate electromagnetic radiation, acoustic signals, or emanations. |
| Simple security property | Bell-LaPadula security model rule allowing a subject read access to an object, only if the security level of the subject dominates the security level of the object. |
| Sniffer | Software tool for auditing and identifying network traffic packets. |
| Software assurance | Level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at anytime during its lifecycle, and that the software functions in the intended manner. |
| Software system test and evaluation process | Process that plans, develops, and documents the quantitative demonstration of the fulfillment of all baseline functional performance, operational, and interface requirements. |
| Special access program (SAP) | Sensitive program, approved in writing by a head of agency with original top secret classification authority, that imposes need-to-know and access controls beyond those normally provided for access to Confidential, Secret, or Top Secret information. The level of controls is based on the criticality of the program and the assessed hostile intelligence threat. The program may be an acquisition program, an intelligence program, or an operations and support program. (Joint Pub 1-02, 12 Apr 2001) |
| Spillage | See classified information spillage. |
| Split knowledge | Separation of data or information into two or more parts, each part constantly kept under control of separate authorized individuals or teams so that no one individual or team will know the whole data. |
| Spoofing | Unauthorized use of legitimate Identification and Authentication (I&A) data, however it was obtained, to mimic a subject different from the attacker. Impersonating, masquerading, piggybacking, and mimicking are forms of spoofing. |
| 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. |
| Storage object | Object supporting both read and write accesses to an information system. |
| Strong authentication | Layered authentication approach relying on two or more authenticators to establish the identity of an originator or receiver of information. |
| Subject | Generally an individual, process, or device causing information to flow among objects or change to the system state. |
| 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. |
| Suppression measure | Action, procedure, modification, or device that reduces the level of, or inhibits the generation of, compromising emanations in an information system. |
| Symmetric key | Encryption methodology in which the encryptor and decryptor use the same key, which must be kept secret. |
| Synchronous crypto-operation | Method of on-line crypto-operation in which crypto-equipment and associated terminals have timing systems to keep them in step. |
| System administrator (SA) | Individual responsible for the installation and maintenance of an information system, providing effective information system utilization, adequate security parameters, and sound implementation of established IA policy and procedures. |
| System assets | Any software, hardware, data, administrative, physical, communications, or personnel resource within an information system. |
| System development | Methodologies developed through software methodologies engineering to manage the complexity of system development. Development methodologies include software engineering aids and high-level design analysis tools. |
| System high | Highest security level supported by an information system. |
| System high mode | Information system 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 | 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 low | Lowest security level supported by 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 | See information systems security. |
| System security engineering | See information systems security engineering. |
| System security officer | See information system security officer. |
| System security plan | Document fully describing the planned security tasks and controls required to meet system security requirements. |

## T

|  |  |
| --- | --- |
| Tampering | Unauthorized modification altering the proper functioning of INFOSEC equipment. |
| Target of evaluation (TOE) | IT product or system and its associated (TOE) administrator and user guidance documentation that is the subject of an evaluation. |
| Technical 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. (NIST Special Pub 800-53.) |
| Technical vulnerability information | Detailed description of a vulnerability to include the implementable steps (such as code) necessary to exploit that vulnerability. |
| Telecommunications | Preparation, transmission, communication, or related processing of information (writing, images, sounds, or other data) by electrical, electromagnetic, electromechanical, electro-optical, or electronic means. |
| TEMPEST | Short name referring to investigation, study, and control of compromising emanations from information system equipment. |
| TEMPEST test | Laboratory or on-site test to determine the nature of compromising emanations associated with an information system. |
| TEMPEST zone | Designated area within a facility where equipment with appropriate TEMPEST characteristics (TEMPEST zone assignment) may be operated. |
| Test key | Key intended for testing of COMSEC equipment or systems. |
| Threat | Any circumstance or event with the potential to adversely impact an information system through unauthorized access, destruction, disclosure, modification of data, and/or denial of service. |
| Threat analysis | Examination of information to identify the elements comprising a threat. |
| Threat assessment | Formal description and evaluation of threat to an information system. |
| 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. |
| Time bomb | Resident computer program that triggers an unauthorized act at a predefined 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 TSP. |
| TOE Security Policy (TSP) | Set of rules that regulate how assets are managed, protected, and distributed within the TOE. |
| 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 (TA) | Study of communications patterns. |
| Traffic-flow security (TFS) | Measure used to conceal the presence of valid messages in an on-line cryptosystem or secure communications system. |
| Transmission security(TRANSEC) | Component of COMSEC resulting from the application of measures designed to protect transmissions from interception and exploitation by means other than cryptanalysis. |
| Trap door | Synonymous with back door. |
| Triple DES | Product cipher that, like DES, operates on 64-bit data blocks. There are several forms, each of which uses the DES cipher 3 times. Some forms use two 56-bit keys, some use three. (See NIST FIPS 46-3 and CNSSAM IA/02-04) |
| Trojan horse | Program containing hidden code allowing the unauthorized collection, falsification, or destruction of information. (See malicious code.) |
| Trusted channel | Means by which a TOE Security Function (TSF) and a remote trusted IT product can communicate with necessary confidence to support the TOE Security Policy (TSP). |
| Trusted computer system | information system employing sufficient hardware and software assurance measures to allow simultaneous processing of a range of classified or sensitive 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 | Method for distributing trusted computing base (TCB) hardware, software, and firmware components that protects the TCB from modification during distribution. |
| Trusted path | Means by which a user and a TOE Security Function (TSF) can communicate with necessary confidence to support the TOE Security Policy (TSP). |
| Trusted recovery | Ability to ensure recovery without compromise after a system failure. |
| Tunneling | 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-person control | 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. |
| Type certification | The certification acceptance of replica information systems based on the comprehensive evaluation of the technical and non-technical security features of an information system and other safeguards, made as part of and in support of the accreditation process, to establish the extent to which a particular design and implementation meet a specified set of security requirements. |
| Type 1 key | Generated and distributed under the auspices of NSA for use in a cryptographic device for the protection of classified and sensitive national security information. |
| Type 1 product | Cryptographic equipment, assembly or component classified or certified by NSA for encrypting and decrypting classified and sensitive national security information when appropriately keyed. Developed using established NSA business processes and containing NSA approved algorithms. Used to protect systems requiring the most stringent protection mechanisms. |
| Type 2 key | Generated and distributed under the auspices of NSA for use in a cryptographic device for the protection of unclassified national security information. |
| Type 2 product | Cryptographic equipment, assembly, or component certified by NSA for encrypting or decrypting sensitive national security information when appropriately keyed. Developed using established NSA business processes and containing NSA approved algorithms. Used to protect systems requiring protection mechanisms exceeding best commercial practices including systems used for the protection of unclassified national security information. |
| Type 3 key | Used in a cryptographic device for the protection of unclassified sensitive information, even if used in a Type 1 or Type 2 product. |
| Type 3 product | Unclassified cryptographic equipment, assembly, or component used, when appropriately keyed, for encrypting or decrypting unclassified sensitive U.S. Government or commercial information, and to protect systems requiring protection mechanisms consistent with standard commercial practices. Developed using established commercial standards and containing NIST approved cryptographic algorithms/modules or successfully evaluated by the National Information Assurance Partnership (NIAP). |
| Type 4 key | Used by a cryptographic device in support of its Type 4 functionality; i.e., any provision of key that lacks U.S. Government endorsement or oversight. |
| Type 4 product | Unevaluated commercial cryptographic equipment, assemblies, or components that neither NSA nor NIST certify for any Government usage. These products are typically delivered as part of commercial offerings and are commensurate with the vendor’s commercial practices. These products may contain either vendor proprietary algorithms, algorithms registered by NIST, or algorithms registered by NIST and published in a FIPS. |

## U

|  |  |
| --- | --- |
| Unauthorized disclosure | Type of event involving exposure of information to individuals not authorized to receive it. |
| Unclassified | Information that has not been determined pursuant to E.O. 12958 or any predecessor order to require protection against unauthorized disclosure and that is not designated as classified. |
| Updating | Automatic or manual cryptographic process that irreversibly modifies the state of a COMSEC key, equipment, device, or system. |
| User | Individual or process authorized to access an information system.  (PKI) Individual defined, registered, and bound to a public key structure by a certification authority (CA). |
| User ID | Unique symbol or character string used by an information system to identify a specific user. |
| User Partnership Program | Partnership between the NSA and a U.S. (UPP) Government agency to facilitate development of secure information system equipment incorporating NSA-approved cryptography. The result of this program is the authorization of the product or system to safeguard national security information in the user’s specific application. |
| User representative | 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. |
| U.S.-controlled facility | Base or building to which access is physically controlled by U.S. individuals who are authorized U.S. Government or U.S. Government contractor employees. |

## V

|  |  |
| --- | --- |
| Validated products list | List of validated products that have been successfully evaluated under the National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS). |
| Validation | Process of applying specialized security test and evaluation procedures, tools, and equipment needed to establish acceptance for joint usage of an information system by one or more departments or agencies and their contractors. |
| Variant | One of two or more code symbols having the same plain text equivalent. |
| Verification | Process of comparing two levels of an information system specification for proper correspondence (e.g., security policy model with top-level specification, top-level specification with source code, or source code with object code). |
| Virtual private network (VPN) | Protected information system link utilizing tunneling, security controls (see information assurance), and endpoint address translation giving the impression of a dedicated line. |
| Virus | Self-replicating, malicious code that attaches itself to an application program or other executable system component and leaves no obvious signs of its presence. |
| Vulnerability | Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited. |
| Vulnerability analysis | Examination of information to identify the elements comprising a vulnerability. |
| Vulnerability assessment | Formal description and evaluation of vulnerabilities of an information system. |

## W

|  |  |
| --- | --- |
| Warm site | A backup site that contains the IT infrastructure (hardware-wise, sometimes application), but not the data. |
| Web risk assessment | Process for ensuring websites are in compliance with applicable policies. |
| Wireless technology | Permits the active or passive transfer of information between separated points without physical connection. Active information transfer may entail a transmit and/or receive emanation of energy, whereas passive information transfer entails a receive-only capability. Currently wireless technologies use IR, acoustic, RF, and optical but, as technology evolves, wireless could include other methods of transmission. |
| Work factor | Estimate of the effort or time needed by a potential perpetrator, with specified expertise and resources, to overcome a protective measure. |
| Worm | See malicious code. |
| 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. |

## Z

|  |  |
| --- | --- |
| Zero fill | To fill unused storage locations in an information system with the representation of the character denoting “0.” |
| Zeroize | To remove or eliminate the key from a cryptoequipmentor fill device. |

# SECTION II: COMMONLY USED ABBREVIATIONS AND ACRONYMS

|  |  |
| --- | --- |
| ACK | Acknowledgement. A packet message used in the Transmission Control Protocol (TCP) to acknowledge receipt of a packet |
| ACL | Access Control List |
| ADSL | Asynchronous Digital Subscriber Line |
| AES | Advanced Encryption Standard |
| AKD/RCU A | Automatic Key Distribution/Rekeying Control Unit |
| ANSI | American National Standards Institute |
| APC | Adaptive Predictive Coding |
| APU | Auxiliary Power Unit |
| ARP / Reverse ARP | Address Resolution Protocol |
| ASCII | American Standard Code for Information Interchange |
| ASSIST | Program Automated Information System Security Incident Support Team Program |
| ATM | Asynchronous Transfer Mode |
| AUTODIN | Automatic Digital Network |
| AVP | Authorized Vendor Program |
| C2 | Command and Control |
| C3 | Command, Control, and Communications |
| C3I | Command, Control, Communications and Intelligence |
| C4 | Command, Control, Communications and Computers |
| C4ISR | Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance |
| CA | 1. Certification Authority  2. Certification Agent |
| C&A | Certification and Accreditation |
| CC | Common Criteria |
| CCEP | Commercial COMSEC Evaluation Program |
| CCEVS | Common Criteria Evaluation and Validation Scheme |
| CCI | Controlled Cryptographic Item |
| CCO | Circuit Control Officer |
| CDMA | Code Division Multiple Access |
| CDS | Cross Domain Solution |
| CERT | Computer Security Emergency Response Team |
| CFD | Common Fill Device |
| CIK | Crypto-Ignition Key |
| CIRT | Computer Security Incident Response Team |
| CISA | Certified Information Security Auditor (A professional certification from ISACA) |
| CISM | Certified Information Security Manager (A professional certification from ISACA) |
| CISSP | Certified Information Systems Security Professional (A professional certification from ISC2) |
| CKG | Cooperative Key Generation |
| CMCS | COMSEC Material Control System |
| CNA | Computer Network Attack |
| CND | Computer Network Defense |
| CNSS | Committee on National Security Systems |
| CNSSAM | Committee on National Security Systems Advisory Memorandum |
| CNSSD | Committee on National Security Systems Directive |
| CNSSI | Committee on National Security Systems Instruction |
| CNSSP | Committee on National Security Systems Policy |
| CO | 1. Commanding Officer  2. Contracting Officer |
| COMPUSEC | Computer Security |
| COMSEC | Communications Security |
| CONOP | Concept of Operations |
| COOP | Continuity of Operations Plan |
| COR | 1. Central Office of Record (COMSEC)  2. Contracting Officer Representative |
| COTR | Contracting Office Technical Representative |
| COTS | Commercial-off-the-shelf |
| CPU | Central Processing Unit |
| CRC | Cyclic Redundancy Check |
| CRL | Certificate Revocation List |
| Crypt/Crypto | Cryptographic-related |
| CSIRC | Computer Security Incident Response Center |
| CSMA | Carrier Sensing Multiple Access |
| CSMA/CD | Carrier Sensing Multiple Access with Collision Detection |
| CSMA/CA | Carrier Sensing Multiple Access with Collision Avoidance |
| CSU/DSU | Channel Service Unit/ Digital Service Unit |
| CT&E | Certification Test and Evaluation |
| CTTA | Certified TEMPEST Technical Authority |
| DAA | 1. Designated Accrediting Authority  2. Delegated Accrediting Authority  3. Designated Approval Authority |
| DAC | Discretionary Access Control |
| DAMA | Demand Assigned Multiple Access |
| DCID | Director Central Intelligence Directive |
| DCS | 1. Defense Communications System  2. Defense Courier Service |
| DDS | Dual Driver Service (courier) |
| DES | Data Encryption Standard |
| DIACAP | DoD Information Assurance Certification and Accreditation Process |
| DISN | Defense Information System Network |
| DITSCAP | DoD Information Technology Security Certification and Accreditation Process |
| DMA | Direct Memory Access |
| DMS | Defense Message System |
| DoD AF | Department of Defense Architecture Framework |
| DS | Digital Signal |
| DSA | Digital Signature Algorithm |
| DSL | Digital Subscriber Line |
| DSN | Defense Switched Network |
| DSVT | Digital Subscriber Voice Terminal |
| DTLS | Descriptive Top-Level Specification |
| DTD | Data Transfer Device |
| DTE/DCE | Data Terminal Equipment/ Data Circuit-terminating Equipment |
| EBCDIC | Extended Binary Coded Decimal Interchange Code |
| ECCM | Electronic Counter-Countermeasures |
| ECM | Electronic Countermeasures |
| ECPL | Endorsed Cryptographic Products List (a section in the Information Systems Security Products and Services Catalogue) |
| EDAC | Error Detection and Correction |
| EFD | Electronic Fill Device |
| EFTO | Encrypt For Transmission Only |
| EKMS | Electronic Key Management System |
| eMASS | Enterprise Mission Assurance Support Service (An automated C&A Tool for DIACAP Implementation) |
| EMSEC | Emission Security |
| EPL | Evaluated Products List (a section in the INFOSEC Products and Services Catalogue) |
| ETPL | Endorsed TEMPEST Products List |
| FIPS | Federal Information Processing Standard |
| FOUO | For Official Use Only |
| FSRS | Functional Security Requirements Specification |
| FTP | File Transfer Protocol |
| GCCS | Global Command and Control System |
| GOTS | Government-off-the-Shelf |
| GPRS | General Packet Radio Service |
| GPS | Global Positioning System |
| GSM | Global System for Mobile communications |
| HDLC | High-level Data Link Control |
| HSSI | High Speed Serial Interface |
| IA | Information Assurance |
| I&A | Identification and Authentication |
| IATO | Interim Approval to Operate |
| IC | Intelligence Community |
| ICMP | Internet Control Messaging Protocol |
| ICU | Interface Control Unit |
| IDS | Intrusion Detection System |
| IEEE | Institute of Electrical and Electronics Engineers |
| IGMP | Internet Group Management Protocol. Created because IPv4 support only unicast and broadcast. IGMP is used for multicast. |
| IETF | Internet Engineering Task Force |
| (ISC)2 | International Information Systems Security Certification Consortium |
| ILS | Integrated Logistics Support |
| INFOSEC | Information Systems Security |
| IO | Information Operations |
| IP | Internet Protocol |
| IPsec | Internet Protocol Security |
| IR | Infra-red |
| IS | Information System |
| ISDN | Integrated Services Digital Network |
| ISO/IEC | International Standards Organization/ International Electrotechnical Commission |
| ISSE | Information Systems Security Engineering |
| ISSM | Information Systems Security Manager |
| ISSO | Information Systems Security Officer |
| IT | Information Technology |
| ITAR | International Traffic in Arms Regulation |
| ITSEC | Information Technology Security Evaluation Criteria |
| IXC | Internet eXchange Carrier |
| KAK | Key-Auto-Key |
| KDC | Key Distribution Center |
| KEK | Key Encryption Key |
| KG | Key Generator |
| KMC | Key Management Center |
| KMI | Key Management Infrastructure |
| KMID | Key Management Identification Number |
| KMODC | Key Management Ordering and Distribution Center |
| KMP | Key Management Protocol |
| KMS | Key Management System |
| KP | Key Processor |
| KPK | Key Production Key |
| KSD | Key Storage Device |
| LLC | Logical Link Control |
| LMD/KP | Local Management Device/Key Processor |
| LSI | Large Scale Integration |
| LXC | Local eXchange Carrier |
| MAC | 1. Mandatory Access Control  2. Message Authentication Code  3. Media Address Code |
| MAN | Metropolitan Area Network |
| MIB | Management Information Base |
| MLS | Multilevel Security |
| MUX | Multiplexer |
| NAC | 1. Network Access Control  2. Network Admission Control |
| NACAM | National COMSEC Advisory Memorandum |
| NACSI | National COMSEC Instruction |
| NACSIM | National COMSEC Information Memorandum |
| NAK | Negative Acknowledge |
| NAT | Network Address Translation |
| NCCD | Nuclear Command and Control Document |
| NCSC | National Computer Security Center |
| NISAC | National Industrial Security Advisory Committee |
| NIST | National Institute of Standards and Technology |
| NLZ | No-Lone Zone |
| NOC | Network Operations Center |
| NSA | National Security Agency |
| NSD | National Security Directive |
| NSDD | National Security Decision Directive |
| NSEP | National Security Emergency Preparedness |
| NSI | National Security Information |
| NSS | National Security System |
| NSTAC | National Security Telecommunications Advisory Committee |
| NSTISSAM | National Security Telecommunications and Information Systems Security Advisory/Information Memorandum |
| NSTISSC | National Security Telecommunications and Information Systems Security Committee |
| NSTISSD | National Security Telecommunications and Information Systems Security Directive |
| NSTISSI | National Security Telecommunications and Information Systems Security Instruction |
| NSTISSP | National Security Telecommunications and Information Systems Security Policy |
| NTCB | Network Trusted Computing Base |
| NTISSAM | National Telecommunications and Information Systems Security Advisory/Information Memorandum |
| NTISSD | National Telecommunications and Information Systems Security Directive |
| NTISSI | National Telecommunications and Information Systems Security Instruction |
| NTISSP | National Telecommunications and Information Systems Security Policy |
| OC | Optical Carrier Level |
| OPCODE | Operations Code |
| OPSEC | Operations Security |
| OTP | One-Time Pad |
| PAA | (PKI) Policy Approving Authority  (IC) Principal Accreditating Authority |
| PC | Personal Computer |
| PCIPB | President’s Critical Infrastructure Protection Board |
| PCMCIA | Personal Computer Memory Card International Association |
| PDA | Personal Digital Assistant |
| PDR | Preliminary Design Review |
| PDS | 1. Protected Distribution Systems  2. Power Distribution Systems |
| PKC | Public Key Cryptography |
| PKCS | Public Key Cryptography Standard |
| PKI | Public Key Infrastructure |
| PPL | Preferred Products List (a section in the INFOSEC Products and Services Catalogue) |
| PSTN | Public Switched Telephone Network |
| RA | Registration Authority |
| RBAC | Role-based Access Control |
| RBOC | Regional Bell Operating Company |
| RF | Radio Frequency |
| RPC | Remote Procedure Call |
| SA | System Administrator |
| SABI | Secret and Below Interoperability |
| SAO | Special Access Office |
| SAP | Special Access Program |
| SBU | Sensitive But Unclassified |
| SCI | Sensitive Compartmented Information |
| SCIF | Sensitive Compartmented Information Facility |
| SDLC | (System/Software) System Development Life Cycle  (Telecom) Synchronous Data Link Control |
| SDSL | Symmetric Digital Subscriber Line |
| SDR | System Design Review |
| SHA | Secure Hash Algorithm |
| SFUG | Security Features Users Guide |
| SI | Special Intelligence |
| SIRC | Security Incident Response Center |
| SIRT | Security Incident Response Team |
| SMDS | (Telecom) Switched Multi-megabit Data Service |
| SONET | Synchronous Optical Network |
| SQL | Structured Query Language |
| SRR | Security Requirements Review |
| SSP | System Security Plan |
| ST&E | Security Test and Evaluation |
| SYN | Synchronization packet in Transmission Control Protocol (TCP) |
| TCB | Trusted Computing Base |
| TCP/IP | Transmission Control Protocol/Internet Protocol |
| TDM | Time Division Multiplex |
| TDMA | Time Division Multiple Access |
| TEP | TEMPEST Endorsement Program |
| TFM | Trusted Facility Manual |
| TLS | Top-Level Specification |
| TOE | Target of Evaluation |
| TPC | Two-Person Control |
| TPEP | Trusted Products Evaluation Program |
| TPI | Two-Person Integrity |
| TRANSEC | Transmission Security |
| TRB | Technical Review Board |
| UA | User Agent |
| UDP | User Datagram Protocol |
| VLAN | Virtual Local Area Network |
| VPN | Virtual Private Network |
| WAN | Wide Area Network |
| WAP | (Telecom) Wireless Application Protocol |

# SECTION III: REFERENCES

|  |
| --- |
| CNSSI 4009, *National Information Assurance (IA) Glossary*, June 2006. |
| *CISSP® All-in-One Exam Guide*, Forth Edition, Shon Harris, The McGraw-Hill Companies, 2008. |
| *Official (ISC)2 ® Guide To The CISSP® CBK* by Harold F. Tipton, et. al., Auerbach Publications, 2006. |
| *Official (ISC)2 ® Guide To The CISSP® Exam* by Susan Hansche, et. al., Auerbach Publications, 2004. |
| NIST SP 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*, April 1998. |
| NIST SP 800-30, *Risk Management Guide for Information Technology Systems*, July 2002. |
| NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, May 2004. |
| NIST SP 800-53, Rev. 2, *Recommended Security Controls for Federal Information Systems*, December 2007. |
| NIST SP 800-64 Rev. 1, *Security Considerations in the Information System Development Life Cycle*, June 2004. |
| NIST SP 800-61, *Computer Security Incident Handling Guide*, January, 2004. |
| NIST SP 800-65, *Integrating IT Security into the Capital Planning and Investment Control Process*, January 2005. |
| NIST SP 800-67, *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*, May 2004. |
| NIST SP 800-77, *Guide to IPsec VPNs*, December 2005. |
| FIPS 46-3, *Data Encryption Standard (DES)*, October 1999. |
| FIPS 140-2, *Security Requirements for Cryptographic Modules*, May 2001. |
| FIPS 180-2, *Secure Hash Standard (SHS)*, August 2002. |
| FIPS 185, *Escrowed Encryption Standard*, February 1994. |
| FIPS 186-2, *Digital Signature Standard (DSS)*, January 2000. |
| FIPS 197, *Advanced Encryption Standard*, November 2001. |
| FIPS 198, *The Keyed-Hashed Message Authentication Code (HMAC)*, March 2002. |
| FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, December 2003. |
| FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006. |
| *Information Assurance Technical Framework (IATF)*, Release 3.1, NSA IA Solutions Technical Directors, September 2002. |
| ISO/IEC 15408-1:2005, *Evaluation Criteria for IT Security – Part 1: Introduction and General Model*, 2005. |
| ISO/IEC 15408-2:2005, *Evaluation Criteria for IT Security – Part 2: Security Functional Requirements*, 2005. |
| ISO/IEC 15408-3:2005, *Evaluation Criteria for IT Security – Part 3: Security Assurance Requirements*, 2005. |
| BS ISO/IEC 17799:2005, *Code of Practice for Information Security Management*, 2005. |
| *Control Objectives for Information and related Technology (COBIT)*, Release 4.0, IT Governance Institute, 2005. |
| ISO/IEC 21827, *Systems Security Engineering – Capability Maturity Model (SSE-CMM®)*, 2002. |
| ISO/IEC 27001, *Information Security Management Systems – Requirements*, 2005. |
| Draft MIL-STD-499C, *Systems Engineering*, Aerospace Corporation, April 15, 2005. |
| ISO/IEC 15288:2008(E), IEEE Std 15288-2008, *Systems and Software Engineering – System Life Cycle Processes*, February 1, 2008. |
| IEEE STD 1220-2005, *IEEE Standard for Application and Management of the Systems Engineering Process*, September 9, 2005. |
| IEEE/EIA 12207.0-1996, *Industrial Implementation of International Standard ISO/IEC 12207:1995* *Software Life Cycle Processes*, March 1998. |
| IEEE/EIA 12207.1-1997, *Industrial Implementation of International Standard ISO/IEC 12207:1995 Software Life Cycle Processes—Life Cycle Data*, April 1998. |
| IEEE/EIA 12207.2-1997, *Industrial Implementation of International Standard ISO/IEC 12207:1995 Software Life Cycle Processes—Implementation Considerations*, April 1998. |
| DoD 5200.28-STD, *Department of Defense Trusted Computer System Evaluation Criteria*, December 1985. (a.k.a. Orange Book). |
| NCSC-TG-003, Version-1 A, *Guide to Understanding Discretionary Access Control in Trusted Systems*, September 30, 1987. (a.k.a. Neo-Orange Book). |
| *Information Technology Security Evaluation Criteria (ITSEC)*, Version 1.2, June 1991. |