CNSS Instruction No. 4009
Revised May 2003

NATIONAL INFORMATION ASSURANCE (IA) GLOSSARY

THIS DOCUMENT PROVIDES MINIMUM STANDARDS. FURTHER IMPLEMENTATION MAY BE REQUIRED BY YOUR DEPARTMENT OR AGENCY.

Committee on National Security Systems

National Manager

FOREWORD

1. The CNSS Glossary Working Group recently convened to review terms submitted by the CNSS membership since the Glossary was last published in September 2000. This edition incorporates those terms.

2. We recognize that, to remain useful, a glossary must be in a continuous state of coordination, and we encourage your review and welcome your comments. The goal of the Glossary Working Group is to keep pace with changes in information assurance terminology and to meet regularly for consideration of comments.

3. The Working Group would like your help in keeping this glossary up to date as new terms come into being and old terms fall into disuse or change meaning. Some terms from the previous version were deleted, others updated or added, and some are identified as candidates for deletion (C.F.D.). If a term you still find valuable and need in your environment has been deleted, please resubmit the term with a definition based on the following criteria: (a) specific relevance to the security of information systems; (b) economy of words; (c) accuracy; and (d) clarity. Use these same criteria to recommend any changes to existing definitions or suggest new terms. In all cases, send your suggestions to the CNSS Secretariat via e-mail or fax at the numbers found below.

4. Representatives of the CNSS may obtain additional copies of this instruction at the address listed below.

/s/
MICHAEL V. HAYDEN
Lieutenant General, USAF

CNSS Secretariat (I42) . National Security Agency . 9800 Savage Road . STE 6716 . Ft Meade MD 20755-6716
(410) 854-6805 . UFAX: (410) 854-6814
nstissc@radium.ncsc.mil

SECTION I

TERMS AND DEFINITIONS

A

A1 (C.F.D.)	Highest level of trust defined in the Orange Book (Department of Defense Trusted Computer System Evaluation Criteria, DoD 5200.28-STD).
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 IS.
access control officer (ACO) (C.F.D.)	Designated individual responsible for limiting access to information systems resources.
access level	Hierarchical portion of the security level used to identify the sensitivity of IS 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 period (C.F.D.)	Segment of time, generally expressed in days or weeks, during which access rights prevail.

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.
accountability	(IS) Process of tracing IS 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.
accounting legend code (ALC)	Numeric code used to indicate the minimum accounting controls required for items of accountable COMSEC material within the COMSEC Material Control System.
accounting number	Number assigned to an item of COMSEC material to facilitate its control.
accreditation	Formal declaration by a Designated Accrediting Authority (DAA) that an IS is approved to operate in a particular security mode at an acceptable level of risk, based on the implementation of an approved set of technical, managerial, and procedural safeguards.
accreditation boundary	See security perimeter.
accreditation package	Product comprised of a System Security Plan (SSP) and a report documenting the basis for the accreditation decision.
accrediting authority	Synonymous with Designated Accrediting Authority (DAA).
add-on security	Incorporation of new hardware, software, or firmware safeguards in an operational IS.

advanced encryption standard (AES)	FIPS approved cryptographic algorithm that is a symmetric block cypher 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 IS of an organization. This notification may include analytical insights into trends, intentions, technologies, or tactics of an adversary targeting ISs.
alert	Notification that a specific attack has been directed at the IS of an organization.
alternate COMSEC custodian	Individual designated by proper authority to perform the duties of the COMSEC custodian during the temporary absence of the COMSEC custodian.
alternative work site	Government-wide, national program allowing Federal employees to work at home or at geographically convenient satellite offices for part of the work week (e.g., telecommuting).
anti-jam	Measures ensuring that transmitted information can be received despite deliberate jamming attempts.
anti-spoof	Measures preventing an opponent's participation in an IS.
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.
assembly	(COMSEC) Group of parts, elements, subassemblies, or circuits that are removable items of COMSEC equipment.
assurance	Measure of confidence that the security features, practices, procedures, and architecture of an IS accurately mediates and enforces the security policy.

attack	Attempt to gain unauthorized access to an IS's services, resources, or information, or the attempt to compromise an IS's integrity, availability, or confidentiality.
Attack Sensing and Warning (AS&W)	Detection, correlation, identification, and characterization of intentional unauthorized activity with notification to decision makers so that an appropriate response can be developed.
attention character (C.F.D.)	In Trusted Computing Base (TCB) design, a character entered from a terminal that tells the TCB the user wants a secure communications path from the terminal to some trusted code to provide a secure service for the user.
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 IS, 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).
automated security monitoring	Use of automated procedures to ensure security controls are not circumvented or the use of these tools to track actions taken by subjects suspected of misusing the IS.
automatic remote rekeying	Procedure to rekey a distant crypto-equipment electronically without specific actions by the receiving terminal operator.
availability	Timely, reliable access to data and information services for authorized users.

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 IS that sets parameters for system or data use.
Bell-La Padula security model (C.F.D.)	Formal-state transition model of a computer security policy that describes a formal set of access controls based on information sensitivity and

	subject authorizations. See star (*) property and simple security property.
benign	Condition of cryptographic data that cannot be compromised by human access.
benign environment	Nonhostile environment that may be protected from external hostile elements by physical, personnel, and procedural security countermeasures.
beyond A1 (C.F.D.)	Level of trust defined by the DoD Trusted Computer System Evaluation Criteria (TCSEC) to be beyond the state-of-the-art technology. It includes all the Al-level features plus additional ones not required at the Al-level.
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.
brevity list	List containing words and phrases used to shorten messages.
browsing	Act of searching through IS 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 IS terminal, whereby the host system disconnects the terminal and reestablishes contact. Synonymous with dial back.
canister	Type of protective package used to contain and dispense key in punched or printed tape form.
capability (C.F.D.)	Protected identifier that both identifies the object and specifies the access rights to be allowed to the subject who possesses the capability. In a capability-based system, access to protected objects such as files is granted if the would-be subject possesses a capability for the object.
cascading	Downward flow of information through a range of security levels greater than the accreditation range of a system network or component.
category	Restrictive label applied to classified or unclassified information to limit access.
CCI assembly	Device embodying a cryptographic logic or other COMSEC design that NSA has approved as a Controlled Cryptographic Item (CCI). It performs the entire COMSEC function, but depends upon the host equipment to operate.
CCI component	Part of a Controlled Cryptographic Item (CCI) that does not perform the entire COMSEC function but depends upon the host equipment, or assembly, to complete and operate the COMSEC function.
CCI equipment	Telecommunications or information handling equipment that embodies a Controlled Cryptographic Item (CCI) component or CCI assembly and performs the entire COMSEC function without dependence on host equipment to operate.
central office of record (COR)	Office of a federal department or agency that keeps records of accountable COMSEC material held by elements subject to its oversight.

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 IS 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)	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 authority workstation (CAW)	Commercial-off-the-shelf (COTS) workstation with a trusted operating system and special purpose application software that is used to issue certificates.
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 IS.
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.
cipher text auto-key (CTAK)	Cryptographic logic that uses previous cipher text to generate a key stream.
ciphony	Process of enciphering audio information, resulting in encrypted speech.
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.
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).
clearing	Removal of data from an IS, its storage devices, and other peripheral devices with storage capacity, in such a way that the data may not be reconstructed using common system capabilities (i.e., keyboard strokes); however, the data may be reconstructed using laboratory methods. Cleared media may be reused at the same classification

	level or at a higher level. Overwriting is one method of clearing.
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 IS life cycle. Closed security is based upon a system's developers, operators, and maintenance personnel having sufficient clearances, authorization, and configuration control.
code	(COMSEC) System of communication in which arbitrary groups of letters, numbers, or symbols represent units of plain text of varying length.
code book	Document containing plain text and code equivalents in a systematic arrangement, or a technique of machine encryption using a word substitution technique.
code group	Group of letters, numbers, or both in a code system used to represent a plain text word, phrase, or sentence.
code vocabulary	Set of plain text words, numerals, phrases, or sentences for which code equivalents are assigned in a code system.
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.
command authority	Individual responsible for the appointment of user representatives for a department, agency, or organization and their key ordering privileges.

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])
common fill device	One of a family of devices developed to read-in, transfer, or store key.
communications cover	Concealing or altering of characteristic communications patterns to hide information that could be of value to an adversary.
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)	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 IS 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 account audit	Examination of the holdings, records, and procedures of a COMSEC account ensuring all accountable COMSEC material is properly handled and safeguarded.
COMSEC aid	COMSEC material that assists in securing telecommunications and is required in the production, operation, or maintenance of COMSEC systems and their components. COMSEC keying material, callsign/frequency systems, and supporting documentation, such as operating and maintenance manuals, are examples of COMSEC aids.
COMSEC boundary	Definable perimeter encompassing all hardware, firmware, and software components performing critical COMSEC functions, such as key generation and key handling and storage.
COMSEC chip set	Collection of NSA approved microchips.
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 end-item	Equipment or combination of components ready for use in a COMSEC application.
COMSEC equipment	Equipment designed to provide security to telecommunications by converting information to a form unintelligible to an unauthorized interceptor and, subsequently, by reconverting such information to its original form for authorized recipients; also, equipment designed specifically to

	aid in, or as an essential element of, the conversion process. COMSEC equipment includes crypto-equipment, crypto-ancillary equipment, cryptoproduction equipment, and authentication equipment.
COMSEC facility	Authorized and approved space used for generating, storing, repairing, or using COMSEC material.
COMSEC incident	See incident.
COMSEC insecurity	COMSEC incident that has been investigated, evaluated, and determined to jeopardize the security of COMSEC material or the secure transmission of information.
COMSEC manager	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, cryptologistic depots, and COMSEC accounts. COMSEC material other than key may be handled through the CMCS.
COMSEC modification	See information systems security equipment modification.
COMSEC module	Removable component that performs COMSEC functions in a telecommunications equipment or system.
COMSEC monitoring	Act of listening to, copying, or recording transmissions of one's own official telecommunications to analyze the degree of security.

COMSEC profile	Statement of COMSEC measures and materials used to protect a given operation, system, or organization.
COMSEC survey	Organized collection of COMSEC and communications information relative to a given operation, system, or organization.
COMSEC system data	Information required by a COMSEC equipment or system to enable it to properly handle and control key.
COMSEC training	Teaching of skills relating to COMSEC accounting, use of COMSEC aids, or installation, use, maintenance, and repair of COMSEC equipment.
concept of operations (CONOP)	Document detailing the method, act, process, or effect of using an IS.
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 IS 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 IS.
confinement channel	See covert channel.
confinement property (C.F.D.)	Synonymous with star (*) property.
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.

contingency plan (C.F.D.)	Plan maintained for emergency response, backup operations, and post-disaster recovery for an IS, to ensure the availability of critical resources and to facilitate the continuity of operations in an emergency situation.
continuity of operations plan (COOP)	Plan for continuing an organization's (usually a 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 protection	The C2 level of protection described in the Trusted Computer System Evaluation Criteria (Orange Book). Its major characteristics are: individual accountability, audit, access control, and object reuse. These characteristics will be embodied in the NSA produced, Controlled Access Protection Profile (and its related follow-on profiles).
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 security mode (C.F.D.)	See multilevel security.
controlled sharing (C.F.D.)	Condition existing when access control is applied to all users and components of an IS.
controlled space	Three-dimensional space surrounding IS 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.
cooperative key generation	Electronically exchanging functions of locally generated, random components, from which both terminals of a secure circuit construct traffic encryption key or key encryption key for use on that circuit.
cooperative remote rekeying	Synonymous with manual remote rekeying.
correctness proof	A mathematical proof of consistency between a specification and its implementation.
countermeasure	Action, device, procedure, technique, or other measure that reduces the vulnerability of an IS.
covert channel	Unintended and/or unauthorized communications path that can be used to transfer information in a manner that violates an IS 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	Those physical and cyber-based systems essential to the minimum operations of the economy and government.
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 equipment room (CER)	Controlled-access room in which cryptosystems are located.
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) crypto-algorithm(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.
cryptonet	Stations holding a common key.
cryptoperiod	Time span during which each key setting remains in effect.
cryptosecurity	Component of COMSEC resulting from the provision of technically sound cryptosystems and their proper use.
cryptosynchronization	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

dangling threat (C.F.D.)	Set of properties about the external environment for which there is no corresponding vulnerability and therefore no implied risk.
dangling vulnerability (C.F.D.)	Set of properties about the internal environment for which there is no corresponding threat and, therefore, no implied risk.
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.
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 IS 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	IS 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, subcompartments, and/or special access programs); and c. valid need-to-know for all information contained within the IS. 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 IS. 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.
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	Type of incident resulting from any action or series of actions that prevents any part of an IS from functioning.
depot maintenance	See full maintenance.
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.
design documentation (C.F.D.)	Set of documents, required for Trusted Computer System Evaluation Criteria (TCSEC) classes C1 and above (as defined in the Orange Book, Department of Defense Trusted Computer System Evaluation Criteria, DoD 5200.28-STD), whose primary purpose is to define and describe the properties of a system. As it relates to TCSEC, design documentation provides an explanation of how the security policy of a system is translated into a technical solution via the Trusted Computing Base (TCB) hardware, software, and firmware.
designated accrediting 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 designated approving authority and delegated accrediting authority.
dial back	Synonymous with call back.
digital signature	Cryptographic process used to assure message originator authenticity, integrity, and nonrepudiation.

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 recover plan	Provides for the continuity of system operations after a disaster.
discretionary access control (DAC)	Means of restricting access to objects based on the 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. It purpose is to enforce the internal network's IA policy for external information exchange and to provide external, untrusted sources with restricted access to releasable information while shielding the internal networks from outside attacks. A DMZ is also called a "screened subnet."
DoD Trusted Computer System Evaluation Criteria (TCSEC) C.F.D.	Document containing basic requirements and evaluation classes for assessing degrees of effectiveness of hardware and software security controls built into an IS. This document, DoD 5200.28 STD, is frequently referred to as the Orange Book.
domain	Unique context (e.g., access control parameters) in which a program is operating; in effect, the set of objects a subject has the privilege to access.
dominate	Term used to compare IS security levels. Security

(C.F.D.)	level S1 is said to dominate security level S2, if the hierarchical classification of S1 is greater than, or equal to, that of S2 and the non-hierarchical categories of S1 include all those of S2 as a subset.
drop accountability	Procedure under which a COMSEC account custodian initially receipts for COMSEC material, and then provides no further accounting for it to its central office of record. Local accountability of the COMSEC material may continue to be required. See accounting legend code.

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

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	Protection resulting from measures taken to deny unauthorized individuals information derived from intercept and analysis of compromising emanations from crypto-equipment or an IS.
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 IS 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 IS for the purpose of detecting attempted penetrations.
environment	Aggregate of external procedures, conditions, and objects affecting the development, operation, and maintenance of an IS.
erasure	Process intended to render magnetically stored information irretrievable by normal means.
Evaluated Products List (EPL) (C.F.D.)	Equipment, hardware, software, and/or firmware evaluated by the National Computer Security Center (NCSC) in accordance with DoD TCSEC and found to be technically compliant at a particular level of trust. The EPL is included in the NSA Information Systems Security Products and Services Catalogue.
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 IS.
executive state	One of several states in which an IS 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 IS and is usable or detectable

	by subjects external to the trusted computing base. See covert channel.
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.

fetch protection (C.F.D.)	IS hardware provided restriction to prevent a program from accessing data in another user's segment of storage.
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 semipermanent 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 IS that may allow protection mechanisms to be bypassed.
flaw hypothesis methodology	System analysis and penetration technique in which the specification and documentation for an IS 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 eligibiity and need-to-know.
formal development methodology	Software development strategy that proves security design specifications.
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 model	Mathematically precise statement of a security policy. Such a model must define a secure state, an initial state, and how the model represents changes in state. The model must be shown to be secure by proving the initial state is secure and all possible subsequent states remain secure.
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 IS 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. Also known as depot maintenance. See limited maintenance.

functional proponent	See network sponsor.
functional testing	Segment of security testing in which advertised security mechanisms of an IS are tested under operational conditions.

G

gateway	Interface providing a compatibility between networks by converting transmission speeds, protocols, codes, or security measures.
global information infrastructure (GII)	Worldwide interconnections of the information systems of all countries, international and multinational organizations, and international commercial communications.
granularity (C.F.D.)	Relative fineness to which an access control mechanism can be adjusted.
guard	Mechanism limiting the exchange of information between systems.
Gypsy verification environment (C.F.D.)	Integrated set of software tools for specifying, coding, and verifying programs written in the Gypsy language.

H

hacker	Unauthorized user who attempts to or gains access to an IS.
handshaking procedures	Dialogue between two IS'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.
hashword	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).

I

IA architecture	Framework that assigns and portrays IA roles and behavior among all IT assets, and prescribes rules for interaction and interconnection.
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 IS uses to recognize an entity.
identity token	Smart card, metal key, or other physical object used to authenticate identity.
identity validation	Tests enabling an IS 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 IS. (COMSEC) Occurrence that potentially jeopardizes the security of COMSEC material or the secure electrical transmission of national security information or information governed by 10 U.S.C. Section 2315.
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 IS.
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 IS 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 ISs while defending one's own information and ISs.
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 acquisiton 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/or remove a potential TEMPEST exploitation exists. Synonymous with zone of control.
integrity	Quality of an IS reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. Note that, in a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information.
integrity check value	Checksum capable of detecting modification of an IS.

interconnection security agreement	Written management authorization to interconnect information systems based upon acceptance of risk and implementatin of established controls.
inter-domain connections	Connections between domains of different classifications for the purpose of transferring data through controlled interfaces.
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 IS lifecycle.
interim approval	Temporary authorization granted by a DAA for an IS to process information based on preliminary results of a security evaluation of the system.
internal security controls	Hardware, firmware, or software features within an IS that restrict access to resources only to authorized subjects.
internetwork private line interface	Network cryptographic unit that provides secure connections, singularly or in simultaneous multiple connections, between a host and a predetermined set of corresponding hosts.
internet protocol (IP)	Standard protocol for transmission of data from source to destinations in packet-switched communications networks and interconnected systems of such networks.
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 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 IS.
level of concern	Rating assigned to an IS 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 IS for confidentiality, integrity, and availability.
level of protection	Extent to which protective measures, techniques, and procedures must be applied to ISs and networks based on risk, threat, vulnerability, system interconnectivity considerations, and information assurance needs. Levels of protection are: 1. Basic: IS and networks requiring implementation of standard minimum security countermeasures. 2. Medium: IS and networks

	requiring layering of additional safeguards above the standard minimum security countermeasures. 3. High: IS 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 IS signal, power, control, indicator, or other external interface line.
line conduction	Unintentional signals or noise induced or conducted on a telecommunications or IS signal, power, control, indicator, or other external interface line.
link encryption	Encryption of information between nodes of a communications system.
list-oriented	IS protection in which each protected object has a list of all subjects authorized to access it. See also ticket-oriented.
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 IS 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 IS.
malicious code	Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an IS.
malicious logic	Hardware, software, or firmware capable of performing an unauthorized function on an IS.
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 deception	Alteration or simulation of friendly telecommunications for the purpose of deception. See communications deception and imitative communications deception.
manual cryptosystem	Cryptosystem in which the cryptographic processes are performed without the use of crypto-equipment or auto-manual devices.
manual remote rekeying	Procedure by which a distant crypto-equipment is rekeyed electrically, with specific actions required by the receiving terminal operator.
masquerading	Form of spoofing.
master crypto-ignition key	Key device with electronic logic and circuits providing the capability for adding more operational CIKs to a keyset (maximum of seven) any time after fill procedure is completed. The master CIK can only be made during the fill procedure as the first CIK.
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	Form of 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 IS 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 IS; 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.
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 ISs 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 amount 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 (NSI)	Information that has been determined, pursuant to Executive Order 12958 or any predecessor order, to require protection against unauthorized disclosure.
national security system	Any telecommunications or information system operated by the United States Government, the function, operation, or use of which: 1. involves intelligence activities; 2. involves cryptologic activities related to national security; 3. involves command and control of military forces; 4. involves equipment that is an integral part of a weapon or weapon system; or 5. is critical to the direct fulfillment of military or intelligence missions and 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 40 U.S.C. Section1452, Information Technology Management Reform Act of 1996.)
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	IS 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 architecture	Subset of network architecture specifically addressing security-relevant issues.
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 trusted computing base (NTCB) (C.F.D.)	Totality of protection mechanisms within a network, including hardware, firmware, and software, the combination of which is responsible for enforcing a security policy. See trusted computing base.
network trusted computing base (NTCB) partition (C.F.D.)	Totality of mechanisms within a single network component for enforcing the network policy, as allocated to that component; the part of the NTCB within a single network component.
network weaving	Penetration technique in which different communication networks are linked to access an IS 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.
nonrepudiation	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.
off-line cryptosystem	Cryptosystem in which encryption and decryption are performed independently of the transmission and reception functions.
one-part code	Code in which plain text elements and their accompanying code groups are arranged in alphabetical, numerical, or other systematic order, so one listing serves for both encoding and decoding. One-part codes are normally small codes used to pass small volumes of low-sensitivity information.
one-time cryptosystem	Cryptosystem employing key used only once.

one-time pad	Manual one-time cryptosystem produced in pad form.
one-time tape	Punched paper tape used to provide key streams on a one-time basis in certain machine cryptosystems.
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 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.

Orange Book (C.F.D)	DoD Trusted Computer System Evaluation Criteria (DoD 5200.28-STD).
organizational maintenance	Limited maintenance performed by a user organization.
organizational registration authority (ORA)	Entity within the PKI that authenticates the identity and the organizational affiliation of the users.
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	IS 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 IS.

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.
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.
preproduction model	Version of INFOSEC equipment employing standard parts and suitable for complete

	evaluation of form, design, and performance. Preproduction models are often referred to as beta models.
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 access (C.F.D.)	Explicitly authorized access of a specific user, process, or computer to a computer resource(s).
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 IS 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 IS 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 that meets specific consumer needs.
protection ring	One of a hierarchy of privileged modes of an IS 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, permiting ISs 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 IS that results only in the flow of information from an object to a subject.
read access	Permission to read information in an IS.
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 IS and computational capability after a system failure.
RED	Designation applied to an IS, 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	Independent and focused threat-based effort by an interdisciplinary, simulated adversary to expose and exploit vulnerabilities as a means to improve the security posture of ISs.
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.
reference validation mechanism	Portion of a trusted computing base whose normal function is to control access between subjects and objects and whose correct operation is essential to the protection of data in the system.
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 IS 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 IS by exploiting a particular vulnerability.
risk analysis	Examination of information to identify the risk to an IS.
risk assessment	Process of analyzing threats to and vulnerabilities of an IS, 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 IS users and the maximum

	sensitivity (e.g., classification and categories) of data processed by the system.
risk management	Process of identifying and applying countermeasures commensurate with the value of the assets protected based on a risk assessment.

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 fault analysis (SFA)	Assessment, usually performed on IS hardware, to determine the security properties of a device when hardware fault is encountered.
security features users guide (SFUG) (C.F.D.)	Guide or manual explaining how the security mechanisms in a specific system work.
security filter	IS trusted subsystem that enforces security policy on the data passing through it.
security inspection	Examination of an IS 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 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	All components/devices of an IS to be accredited. Separately accredited components generally are not included within the perimeter.
security range	Highest and lowest security levels that are permitted in or on an IS, system component, subsystem, or network.
security requirements	Types and levels of protection necessary for equipment, data, information, applications, and facilities to meet IS security policy.

security requirements baseline	Description of the minimum requirements necessary for an IS to maintain an acceptable level of security.
security safeguards	Protective measures and controls prescribed to meet the security requirements specified for an IS. 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 IS.
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 IS, as they have been applied in an operational environment, to determine the security posture of that system.
security testing	Process to determine that an IS 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.
shielded enclosure	Room or container designed to attenuate electromagnetic radiation.
short title	Identifying combination of letters and numbers assigned to certain COMSEC materials to facilitate handling, accounting, and controlling.
simple security property (C.F.D.)	Bell-La Padula 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.
single point keying	Means of distributing key to multiple, local crypto-equipment or devices from a single fill point.
sniffer	Software tool for auditing and identifying network traffic packets.
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)	Program established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classified level.
special access program facility (SAPF)	Facility formally accredited by an appropriate agency in accordance with DCID 1/21 in which SAP information may be procesed.

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 Indentification 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.
star (*) property (C.F.D.)	Bell-La Padula security model rule allowing a subject write access to an object only if the security level of the object dominates the security level of the subject.
start-up KEK	Key-encryption-key held in common by a group of potential communicating entities and used to establish ad hoc tactical networks.
state variable	Variable representing either the state of an IS or the state of some system resource.
storage object	Object supporting both read and write accesses to an IS.
strong authentication	Layered authentication approach relying on two or more authenticators to establish the identity of an originator or receiver of information.
subassembly	Major subdivision of an assembly consisting of a package of parts, elements, and circuits that perform a specific function.
subject	Generally an individual, process, or device causing information to flow among objects or 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.
superencryption	Process of encrypting encrypted information. Occurs when a message, encrypted off-line, is transmitted over a secured, on-line circuit, or when information encrypted by the originator is multiplexed onto a communications trunk, which is then bulk encrypted.
supersession	Scheduled or unscheduled replacement of a COMSEC aid with a different edition.
supervisor state	Synonymous with executive state of an operating system.
suppression measure	Action, procedure, modification, or device that reduces the level of, or inhibits the generation of, compromising emanations in an IS.
surrogate access	See discretionary access control.
syllabary	List of individual letters, combination of letters, or syllables, with their equivalent code groups, used for spelling out words or proper names not present in the vocabulary of a code. A syllabary may also be a spelling table.
symmetric 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 IS, providing effective IS 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 IS.
system development methodologies	Methodologies developed through software engineering to manage the complexity of system development. Development methodologies include software engineering aids and high-level design analysis tools.
system high	Highest security level supported by an IS.
system high mode	IS security mode of operation wherein each user, with direct or indirect access to the IS, its peripherals, remote terminals, or remote hosts, has all of the following: a. valid security clearance for all information within an IS; b. formal access approval and signed nondisclosure agreements for all the information stored and/or processed (including all compartments, subcompartments and/or special access programs); and c. valid need-to- know for some of the information contained within the IS.
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 IS 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 IS.
system profile	Detailed security description of the physical structure, equipment component, location, relationships, and general operating environment of an IS.
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	Formal document fully describing the planned security tasks required to meet system security requirements.

T

tampering	Unauthorized modification altering the proper functioning of INFOSEC equipment.
target of evaluation	IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.
telecommunications	Preparation, transmission, communication, or related processing of information (writing, images, sounds, or other data) by electrical, electromagnetic, electromechanical, electro-optical, or electronic means.
telecommunications security (TSEC) (C.F.D.)	See information systems security.
TEMPEST	Short name referring to investigation, study, and control of compromising emanations from IS equipment.
TEMPEST test	Laboratory or on-site test to determine the nature of compromising emanations associated with an IS.
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 IS 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 IS.
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.
ticket-oriented	IS protection system in which each subject maintains a list of unforgeable bit patterns called tickets, one for each object a subject is authorized to access. See list-oriented.
time bomb	Resident computer program that triggers an unauthorized act at a predefined time.
time-compliance date	Date by which a mandatory modification to a COMSEC end-item must be incorporated if the item is to remain approved for operational use.
time-dependent password	Password that is valid only at a certain time of day or during a specified interval of time.
TOE Security Functions (TSF)	Set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the 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 encryption key (TEK)	Key used to encrypt plain text or to superencrypt previously encrypted text and/or to decrypt cipher text.
traffic-flow security (TFS)	Measure used to conceal the presence of valid messages in an on-line cryptosystem or secure communications system.
traffic padding	Generation of spurious communications or data units to disguise the amount of real data units being sent.
tranquility	Property whereby the security level of an object cannot change while the object is being processed by an IS.
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.
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	IS 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 facility manual (C.F.D.)	Document containing the operational requirements; security environment; hardware and software configurations and interfaces; and all security procedures, measures, and contingency plans.
trusted identification forwarding	Identification method used in IS networks whereby the sending host can verify an authorized user on its system is attempting a connection to another host. The sending host transmits the required user authentication information to the receiving host.
trusted path	Means by which a user and a TOE Security Function (TSF) can communicate with necessary confidence to support the TOE Security Policy (TSP).
trusted process	Process that has privileges to circumvent the system security policy and has been tested and verified to operate only as intended.
trusted recovery	Ability to ensure recovery without compromise after a system failure.
trusted software	Software portion of a trusted computing base (TCB).
TSEC nomenclature	System for identifying the type and purpose of certain items of COMSEC material.
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-part code	Code consisting of an encoding section, in which the vocabulary items (with their associated code groups) are arranged in alphabetical or other systematic order, and a decoding section, in which the code groups (with their associated meanings) are arranged in a separate alphabetical or numeric order.
two-person control	Continuous surveillance and control of positive control material at all times by a minimum of two

	authorized individuals, each capable of detecting incorrect and unauthorized procedures with respect to the task being performed, and each familiar with established security and safety requirements.
two-person integrity (TPI)	System of storage and handling designed to prohibit individual access to certain COMSEC keying material by requiring the presence of at least two authorized individuals, each capable of detecting incorrect or unauthorized security procedures with respect to the task being performed. See no-lone zone.
type certification	The certification acceptance of replica information systems based on the comprehensive evaluation of the technical and non-technical security features of an IS 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 product	Classified or controlled cryptographic item endorsed by the NSA for securing classified and sensitive U.S. Government information, when appropriately keyed. The term refers only to products, and not to information, key, services, or controls. Type 1 products contain approved NSA algorithms. They are available to U.S. Government users, their contractors, and federally sponsored non-U.S. Government activities subject to export restrictions in accordance with International Traffic in Arms Regulation.
type 2 product	Unclassified cryptographic equipment, assembly, or component, endorsed by the NSA, for use in national security systems as defined in Title 40 U.S.C. Section 1452.
type 3 algorithm	Cryptographic algorithm registered by the National Institute of Standards and Technology (NIST) and published as a Federal Information Processing Standard (FIPS) for use in protecting unclassified sensitive information or commercial information.

type 4 algorithm	Unclassified cryptographic algorithm that has been registered by the National Institute of Standards and Technology (NIST), but not published as a Federal Information Processing Standard (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.
untrusted process	Process that has not been evaluated or examined for adherence to the security policy. It may include incorrect or malicious code that attempts to circumvent the security mechanisms.
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 IS. (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 IS to identify a specific user.
User Partnership Program (UPP)	Partnership between the NSA and a U.S. Government agency to facilitate development of secure IS 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.
U.S.-controlled space	Room or floor within a facility that is not a U.S.-controlled facility, access to which is physically controlled by U.S. individuals who are authorized U.S. Government or U.S. Government contractor employees. Keys or combinations to locks controlling entrance to U.S.-controlled spaces must be under the exclusive control of U.S. individuals who are U.S. Government or U.S. Government contractor employees.
U.S. person	U.S. citizen or a permanent resident alien, an unincorporated association substantially composed of U.S. citizens or permanent resident aliens, or a corporation incorporated in U.S., except for a corporation directed and controlled by a foreign government or governments.

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 IS 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 IS 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 IS link utilizing tunneling, security controls (see information assurance), and end-point 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 IS, 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 IS.

W

web risk assessment	Process for ensuring websites are in compliance with applicable policies.
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 IS 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 IS.

Z

zero fill	To fill unused storage locations in an IS with the representation of the character denoting "0."
zeroize	To remove or eliminate the key from a crypto-equipment or fill device.
zone of control	Synonymous with inspectable space.

SECTION II

COMMONLY USED ABBREVIATIONS AND ACRONYMS

ACL	Access Control List
ACO (C.F.D.)	Access Control Officer
AES	Advanced Encryption standard
AIG	Address Indicator Group
AIN	Advanced Intelligence Network
AK	Automatic Remote Rekeying
AKD/RCU	Automatic Key Distribution/Rekeying Control Unit
ALC	Accounting Legend Code
AMS	1. Auto-Manual System 2. Autonomous Message Switch
ANDVT	Advanced Narrowband Digital Voice Terminal
ANSI	American National Standards Institute
APC	Adaptive Predictive Coding
APU	Auxiliary Power Unit
ASCII	American Standard Code for Information Interchange
ASSIST Program	Automated Information System Security Incident Support Team Program
ASU (C.F.D.)	Approval for Service Use
ATM	Asynchronous Transfer Mode
AUTODIN	Automatic Digital Network
AVP	Authorized Vendor Program

C2	1. Command and Control 2. Controlled Access Protection (C.F.D.)
C3	Command, Control, and Communications
C3I	Command, Control, Communications and Intelligence
C4	Command, Control, Communications and Computers
CA	1. Controlling Authority 2. Cryptanalysis 3. COMSEC Account 4. Command Authority 5. Certification Authority
C&A	Certification and Accreditation
CAW	Certificate Authority Workstation
CC	Common Criteria
CCEP	Commercial COMSEC Evaluation Program
CCEVS	Common Criteria Evaluation and Validation Scheme
CCI	Controlled Cryptographic Item
CCO	Circuit Control Officer
CEOI	Communications Electronics Operating Instruction
CEPR	Compromising Emanation Performance Requirement
CER	1. Cryptographic Equipment Room 2. Communication Equipment Room
CERT	Computer Security Emergency Response Team
CFD	Common Fill Device
CIAC	Computer Incident Assessment Capability
CIK	Crypto-Ignition Key

CIRT	Computer Security Incident Response Team
CKG	Cooperative Key Generation
CMCS	COMSEC Material Control System
CNA	Computer Network Attack
CNCS (C.F.D.)	Cryptonet Control Station
CND	Computer Network Defense
CNK (C.F.D.)	Cryptonet Key
CNSS	Committee on National Security Systems
COMPUSEC	Computer Security
COMSEC	Communications Security
CONOP	Concept of Operations
COOP	Continunity of Operations Plan
COR	1. Central Office of Record (COMSEC) 2. Contracting Officer Representative
COTS	Commercial-off-the-shelf
CPS (C.F.D.)	COMSEC Parent Switch
CPU	Central Processing Unit
CRL	Certificate Revocation List
CRP (C.F.D.)	COMSEC Resources Program (Budget)
Crypt/Crypto	Cryptographic-related
CSE	Communications Security Element
CSS	1. COMSEC Subordinate Switch 2. Constant Surveillance Service (Courier) 3. Continuous Signature Service (Courier) 4. Coded Switch System
CSSO	Contractor Special Security Officer

CSTVRP	Computer Security Technical Vulnerability Report Program
CTAK	Cipher Text Auto-Key
CT&E	Certification Test and Evaluation
CTTA	Certified TEMPEST Technical Authority
CUP	COMSEC Utility Program
DAA	1. Designated Accrediting Authority 2. Delegated Accrediting 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
DISN	Defense Information System Network
DITSCAP	DoD Information Technology Security Certification and Accreditation Process
DoD TCSEC (C.F.D.)	Department of Defense Trusted Computer System Evaluation Criteria
DMA	Direct Memory Access
DMS	Defense Message System
DSA	Digital Signature Algorithm
DSN	Defense Switched Network
DSVT	Digital Subscriber Voice Terminal
DTLS	Descriptive Top-Level Specification
DTD	Data Transfer Device

DTS	Diplomatic Telecommunications Service
DUA	Directory User Agent
EAM	Emergency Action Message
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
ELINT	Electronic Intelligence
E Model	Engineering Development Model
EPL	Evaluated Products List (a section in the INFOSEC Products and Services Catalogue)
ERTZ	Equipment Radiation TEMPEST Zone
ETPL	Endorsed TEMPEST Products List
FDIU	Fill Device Interface Unit
FIPS	Federal Information Processing Standard
FOCI	Foreign Owned, Controlled or Influenced
FOUO	For Official Use Only
FSRS	Functional Security Requirements Specification
FSTS	Federal Secure Telephone Service
FTS	Federal Telecommunications System
FTAM	File Transfer Access Management

FTLS	Formal Top-Level Specification
GCCS	Global Command and Control System
GETS	Government Emergency Telecommunications Service
GOTS	Government-off-the-Shelf
GPS	Global Positioning System
GTS	Global Telecommunications Service
GWEN	Ground Wave Emergency Network
IA	Information Assurance
I&A	Identification and Authentication
IBAC	Identity Based Access Control
ICU	Interface Control Unit
IDS	Intrusion Detection System
IEMATS	Improved Emergency Message Automatic Transmission System
IFF	Identification, Friend or Foe
IFFN	Identification, Friend, Foe, or Neutral
ILS	Integrated Logistics Support
INFOSEC	Information Systems Security
IO	Information Operations
IP	Internet Protocol
IPM	Interpersonal Messaging
IPSO	Internet Protocol Security Option
IS	Information System
ISDN	Integrated Services Digital Network
ISO	International Standards Organization

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
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
LEAD	Low-Cost Encryption/Authentication Device
LMD	Local Management Device
LMD/KP	Local Management Device/Key Processor
LOCK	Logical Co-Processing Kernel
LPC	Linear Predictive Coding

LPD	Low Probability of Detection
LPI	Low Probability of Intercept
LRIP	Limited Rate Initial Preproduction
LSI	Large Scale Integration
MAC	1. Mandatory Access Control 2. Message Authentication Code
MAN	1. Mandatory Modification 2. Metropolitan Area Network
MER	Minimum Essential Requirements
MHS	Message Handling System
MI	Message Indicator
MIB	Management Information Base
MIJI (C.F.D.)	Meaconing, Intrusion, Jamming, and Interference
MINTERM	Miniature Terminal
MISSI	Multilevel Information Systems Security Initiative
MLS	Multilevel Security
MSE	Mobile Subscriber Equipment
NACAM	National COMSEC Advisory Memorandum
NACSI	National COMSEC Instruction
NACSIM	National COMSEC Information Memorandum
NAK	Negative Acknowledge
NCCD	Nuclear Command and Control Document
NCS	1. National Communications System 2. National Cryptologic School 3. Net Control Station
NCSC	National Computer Security Center
NISAC	National Industrial Security Advisory Committee

NIST	National Institute of Standards and Technology
NLZ	No-Lone Zone
NSA	National Security Agency
NSD	National Security Directive
NSDD	National Security Decision Directive
NSEP	National Security Emergency Preparedness
NSI	National Security Information
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 Committe
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
NTIA	National Telecommunications and Information Administration
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
OADR	Originating Agency's Determination Required
OPCODE	Operations Code
OPSEC	Operations Security
ORA	Organizational Registration Authority
OTAD	Over-the-Air Key Distribution
OTAR	Over-the-Air Rekeying
OTAT	Over-the-Air Key Transfer
OTP	One-Time Pad
OTT	One-Time Tape
PAA	Policy Approving Authority
PAL	Permissive Action Link
PC	Personal Computer
PCA	Policy Certification Authority
PCIPB	President's Critical Infrastructure Protection Board
PCMCIA	Personal Computer Memory Card International Association
PDR	Preliminary Design Review
PDS	1. Protected Distribution Systems 2. Practices Dangerous to Security
PES	Positive Enable System
PKC	Public Key Cryptography
PKI	Public Key Infrastructure
PKSD	Programmable Key Storage Device
P model	Preproduction Model

PNEK	Post-Nuclear Event Key
PPL	Preferred Products List (a section in the INFOSEC Products and Services Catalogue)
PRBAC (C.F.D.)	Partition Rule Base Access Control
PROPIN	Proprietary Information
PWDS	Protected Wireline Distribution System
RAMP	Rating Maintenance Program
SA	System Administrator
SABI	Secret and Below Interoperability
SAO	Special Access Office
SAP	1. System Acquisition Plan 2. Special Access Program
SARK	SAVILLE Advanced Remote Keying
SBU	Sensitive But Unclassified
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facility
SDNS	Secure Data Network System
SDR	System Design Review
SFA	Security Fault Analysis
SHA	Secure Hash Algorithm
SFUG	Security Features Users Guide
SI	Special Intelligence
SISS	Subcommittee on Information Systems Security
SMU	Secure Mobile Unit
SPK	Single Point Key(ing)
SRR	Security Requirements Review

SSO	Staff Security Officer
SSP	System Security Plan
ST&E	Security Test and Evaluation
STE	Secure Terminal Equipment
STS	Subcommittee on Telecommunications Security
STU	Secure Telephone Unit
TA	Traffic Analysis
TACTERM	Tactical Terminal
TAG	TEMPEST Advisory Group
TCB	Trusted Computing Base
TCP/IP	Transmission Control Protocols
TED	Trunk Encryption Device
TEK	Traffic Encryption Key
TEP	TEMPEST Endorsement Program
TFM	Trusted Facility Manual
TFS	Traffic Flow Security
TLS	Top-Level Specification
TPC	Two-Person Control
TPEP	Trusted Products Evaluation Program
TPI	Two-Person Integrity
TRANSEC	Transmission Security
TRB	Technical Review Board
TRI-TAC	Tri-Service Tactical Communications System
TSABI	Top Secret and Below Interoperability
TSCM	Technical Surveillance Countermeasures

TSEC	Telecommunications Security
TTAP	Trust Technology Assessment Program
UA	User Agent
UIRK (C.F.D.)	Unique Interswitch Rekeying Key
UIS	User Interface System
UPP	User Partnership Program
USDE (C.F.D.)	Undesired Signal Data Emanations
V model (C.F.D.)	Advanced Development Model
VPN	Virtual Private Network
XDM/X Model (C.F.D.)	Experimental Development Model/Exploratory Development Model

SECTION III

REFERENCES

a. National Security Directive 42, National Policy for the Security of National Security Telecommunications and Information Systems, 5 July 1990.

b. Executive Order 12958, National Security Information, dated 29 September 1995.

c. Executive Order 12333, United States Intelligence Activities, dated 4 December 1981.

d. Public Law 100-235, Cmputer Security Act of 1987, dated 8 January 1988.

e. 10 United States Codes Section 2315.

f. 44 United States Code Section 3502(2), Public Law 104-13, Paperwork Reduction Act of 1995, dated 22 May 1995.

g. Information Technology Management Reform Act of 1996 (within Public Law 104-106, DoD Authorization Act of 1996).

h. NSA Information Systems Security Organization Regulation 90-16, dated 29 October 1996.

i. Federal Information Processing Standards Publication 46-2, Data Encryption Standard, dated 30 December 1993.

j. Federal Information Processing Standards Publication 140 Security Requirments for Cryptographic Modules, dated 10 October 2001.

k. Title 40 United States Code Section 1452, National Security System Defined.

l. Title 5 United States Code Section 552a, The Privacy Act, Records Maintained on Individuals.

m. Executive Order (E.O.) 13231, Critical Infrastructure Protection in the Information Age, 16 October 2001.

n. P.O. 107-347, E-Government Act of 2002, Title III, Federal Information Security Management Act (FISMA) of 2002, dated 17 December 2002.

o. International Standard of Common Criteria for Information Technology Security Evaluation 15408, dated August 1999