



TERMS, ABBREVIATIONS, AND ACRONYMS

MODULE 02

INFORMATION SYSTEMS SECURITY (INFOSEC) PROGRAM GUIDELINES

0515-LP-208-8205

Distribution: Submit requests for placement on distribution (including supporting justification), or amendment to the existing distribution, to:

Commanding Officer
NISE East Det. Washington
Code 011C
3801 Nebraska Avenue, N.W.
Washington, DC 20393-5454

Commercial (202) 764-0538
DSN 764-0538

Stocked: Additional copies of NAVSO P-5239-02 can be obtained from the Navy Aviation Supply Office (Code 1013), 5801 Tabor Avenue, Philadelphia PA 19120-5099, through normal supply channels in accordance with NAVSUP P600 (CD-ROM only), using AUTODIN, DAMES, or MILSTRIP message format to DAAS, Dayton, OH.

Cite stock number 0515-LP-208-8205.

Local reproduction is authorized.

DEPARTMENT OF THE NAVY

NAVAL INFORMATION SYSTEMS MANAGEMENT CENTER
ARLINGTON, VA 22202-4311

NAVSO P-5239-02
JUNE 1995

FOREWORD

Navy Staff Publication (NAVSO Pub) 5239, "Information Systems Security (INFOSEC) Program Guidelines" is issued by the Naval Information Systems Management Center. It consists of a series of modules providing procedural, technical, administrative and/or supplemental guidance for all information systems, whether business or tactical, used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or receipt of data. Each module will focus on a distinct program element and describes a standard methodology for planning, implementing and executing that element of the INFOSEC program within the Department of the Navy (DON).

This module, "Terms, Abbreviations, and Acronyms", provides the Information Systems Security Manager (ISSM) and system users with a listing of INFOSEC terms, abbreviations, and acronyms and their meanings which have been standardized for use within the DON. This document is divided into three sections: Section I contains terms and definitions; Section II is a list of commonly used abbreviations and acronym expansions; and Section III contains applicable references.

J. G. HEKMAN
Rear Admiral, SC, USN

NAVSO P-5239-02
JUNE 1995

THIS PAGE INTENTIONALLY BLANK

SECTION I
TERMS AND DEFINITIONS

A

access	<p>(COMSEC) Capability and opportunity to gain knowledge of or to alter information or material.</p> <p>(IS) Ability and means to communicate with (i.e. input to or receive output from), or otherwise make use of any information, resource, or component in an IS.</p> <p>NOTE: An individual does not have "access" if the proper authority or a physical, technical, or procedural measure prevents them from obtaining knowledge or having an opportunity to alter information, material, resources, or components. [G].</p>
access control	<p>Process of limiting access to the resources of an IS only to authorized users, programs, processes, or other systems. [G].</p>
access control list	<p>1. Mechanism implementing discretionary access control in an IS that identifies the users who may access an object and the type of access to the object that a user is permitted. [G].</p> <p>2. Implementation of a matrix, where the columns represent users, the rows represent protected objects, and each cell indicates the type of access to be granted for the associated subject-object pair. [H].</p>
access control mechanism	<p>Security safeguards designed to detect and prevent unauthorized access, and to permit authorized access in an IS. [G].</p>

access level	<p>Hierarchical portion of the security level used to identify the sensitivity of IS data and the clearance or authorization of users.</p> <p>NOTE: Access level, in conjunction with the non-hierarchical categories, forms the sensitivity label of an object. (See category.) [G].</p>
access list	<p>(COMSEC) Roster of persons authorized admittance to a controlled area.</p> <p>(IS) Compilation of users, programs, and/or processes and the access levels and types to which each is authorized. [G].</p>
access mode	<p>The type of access right to an object (e.g., read, write, execute, append, modify, delete, or create). [J].</p>
access period	<p>Segment of time, generally expressed in days or weeks, during which access rights prevail. [G].</p>
access port	<p>Logical or physical identifier a computer uses to distinguish different terminal input/output data streams or the physical connection for attaching an external device. [G].</p>
access type	<p>Privilege to perform an action on a program or file.</p> <p>NOTE: Read, write, execute, append, modify, delete, and create are examples of access types. [G].</p>
accessible space	<p>Area within which the user is aware of all persons entering and leaving, which denies the opportunity for concealed TEMPEST surveillance, and which delineates the closest point of potential TEMPEST intercept. [G].</p>
accountability	<p>(COMSEC) Principle that an individual is responsible for safeguarding and controlling COMSEC equipment, keying material, and information entrusted to his/her care and is answerable to proper authority for the loss or misuse of that equipment or information. [G].</p> <p>(IS) Property that allows auditing of activities on an IS to be traced to persons who may then be held responsible for their actions. [G].</p>
accounting legend code	<p>Numeric code used to indicate the minimum accounting controls required for items of accountable</p>

NAVSO P-5239-02
JUNE 1995

COMSEC material within the COMSEC Material Control System.

NOTE: National-level accounting legend codes are:

ALC-1 - continuously accountable by serial number.

ALC-2 - continuously accountable by quantity. [G].

ALC-3 - COMSEC material is locally accountable by serial number and handled/safeguarded based on its classification after initial receipt to DCMS.

(Note: Assigned to COMSEC keying in lieu of ALC-1 when tactical or operational need dictates decentralized accounting)

ALC-4 - report of initial receipt required. After acknowledging receipt, users may control in accordance with Service, department, or agency directives. [G].

accounting number

Number assigned to an item of COMSEC material to facilitate its control. [G].

accreditation approval

Formal declaration by a designated approving authority that an IS is approved to: (1) operate in a particular security mode; (2) using a prescribed set of safeguards; [G] (3) against a defined threat and with stated vulnerabilities and countermeasures; (4) with a given operational concept; (5) with stated interconnections to other ISs; (6) at an acceptable level of risk for which the accrediting authority has formally assumed responsibility; and (7) for a specific period of time. [L].

accreditation authority

Synonymous with designated approving authority. [G].

accreditation package

A product of the certification effort and the main basis for the accreditation decision.

Note: The accreditation package, at a minimum, will include a recommendation for the accreditation decision and a statement of residual risk in operating the system in its environment. Other information included may vary depending on the system and/or the DAA. [K].

accreditation range

Of a host with respect to a particular network, is a mandatory access control levels for data storage, processing, and transmission. The accreditation will generally reflect the sensitivity level of data that the

	<p>accreditation authority believes the host can reliably keep segregated with an acceptable level of risk in the context of the particular network for which the accreditation range is given. Thus, although a host system might be accredited to employ the mandatory access control levels Confidential, Secret, and Top Secret in stand-alone operation, it might have an accreditation range consisting of the single value Top Secret for attachment to some network. [J].</p>
add-on security	<p>Incorporation of new hardware, software, or firmware safeguards in an operational IS. [G].</p>
administrative security	<p>The management constraints and supplemental controls established to provide an acceptable level of protection for a system. Synonymous with procedural security. [K].</p>
adversary	<p>Person or organization that must be denied access to critical information. [G].</p>
adverse information	<p>Any information that adversely reflects on the integrity or character of a cleared employee, which suggests that his or her ability to safeguard classified information may be impaired or that his or her access to classified information clearly may not be in the interest of national security. The following are examples of adverse information that shall be reported: criminal activities; treatment for mental or emotional disorders; excessive use of intoxicants; use of illegal, controlled substances such as marijuana, heroin, cocaine, and hashish; and excessive indebtedness or recurring financial difficulties. [J].</p>
affirm	<p>A formal methodology developed at the University of Southern California Information Science Institute (USC-ISI) for the specification and verification of abstract data types, incorporating algebraic specification techniques and hierarchical development. [J].</p>
aggregation	<p>A circumstance in which a collection of individuals pieces of information must be classified at a higher level than any single piece of information which comprises it. The higher sensitivity level of the collection results from the sensitivity of the associations between the individual pieces. See Inference. [J].</p>
alternate COMSEC custodian	<p>Person designated by proper authority to perform the duties of the COMSEC custodian during the temporary absence of the COMSEC custodian. [G].</p>

anti-jam	Measures to ensure that intended transmitted information can be received despite deliberate jamming attempts. [G].
anti-spoof	Measures to prevent an opponent's participation in a telecommunications network or operation/control of a cryptographic or COMSEC system. [G].
approval to operate	Concurrence by the DAA that a satisfactory level of security has been provided (minimum requirements are met and there is an acceptable level of risk). It authorizes the operation of an automated system or network at a computer facility. Approval results from an analysis of the computer facility, automated system, and automatic data system certification and the operational environment of the automated system entity by the DAA. [J].
assembly	Group of parts, elements, subassemblies, or circuits that are removable items of COMSEC equipment. [G].
assessment	See risk assessment. [G].
assurance	Measure of confidence that the security features and architecture of an IS accurately mediate and enforce the security policy. [G]. If the security features of an IS are relied on to protect classified or sensitive unclassified information and restrict user access, the features must at least be tested to ensure that the security policy is enforced and may not be circumvented during IS operation. [L].
asymmetric encryption	See Public Key Cryptography. [J].
attack	Act of trying to defeat IS safeguards. [G].
attention character	In TCB design, a character that, when entered from a terminal, signals the TCB that a user wants a secure communication path from the terminal to some trusted code in order to provide a secure service for the user, such as logging in or logging out. [J].
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. [G].

audit trail	<p>1. Chronological record of system activities to enable the reconstruction and examination of the sequence of events and/or changes in an event. [G].</p> <p>2. Provides a mechanism for tracking user activities. [H].</p> <p>NOTE: Audit trail may apply to information in an IS, to message routing in a communications system, or to the transfer of COMSEC material. [G].</p>
authenticate	<p>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 automated information system, or establish the validity of a transmitted message. [G].</p>
authentication	<p>1. Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's eligibility to receive specific categories of information. [G].</p> <p>2. The computer will first identify a user, typically through a logon id, and then the computer system will authenticate the users identity. A wide variety of authentication mechanisms exist, but the most common is a password. [H].</p>
authentication system	<p>Cryptosystem or process used for authentication. [G].</p>
authenticator	<p>Means used to confirm the identity or eligibility of a station, originator, or individual. [G].</p>
authenticity	<p>The service that ensures that system events are initiated by and traceable to authorized entities. It is composed of authentication and nonrepudiation. [K].</p>
authorization	<p>Access rights granted to a user, program, or process. [G].</p>
authorized person	<p>A person who has a need-to-know for classified information in the performance of official duties and who has been granted a personnel clearance at the required level. The responsibility for determining whether a prospective recipient is an "authorized person" rest with the person who has possession, knowledge, or control of the classified information involved, and not with the prospective recipient. [J].</p>

Automated Data Processing (ADP)	Data processing in an automated fashion(i.e., on a computer). See (A)IS. [J].
automated data processing security	Synonymous with (Automated) Information System Security. [J].
(Automated) Information System ((A)IS)	An assembly of computer hardware, software and/or firmware configured to collect, create, communicate, compute, disseminate, process, store, and/or control data or information. [J].
automated information system security	Measures and controls that safeguard or protect an security (A)IS against unauthorized (accidental or intentional) disclosure, modification, or destruction of (A)ISs and data, and denial of service. (A)IS security includes consideration of all hardware and/or software functions, characteristics and /or features; operational procedures, accountability procedures, and access controls at the central computer facility, remote computer, and devices; and personnel and communication controls needed to provide an acceptable level of risk for the (A)IS and for the data and information contained in the (A)IS. It includes the totality of security safeguards needed to provide an acceptable protection level for an (A)IS and for data handled by an (A)IS. [J].
authorized vendor	Manufacturer of existing COMSEC equipment who is authorized to produce quantities in excess of contractual requirements for direct sale to eligible buyers. [G].
Authorized Vendor Program	Program in which a vendor, producing a COMSEC product under contract to the National Security Agency, is authorized to produce that product in numbers exceeding the contracted requirements for direct marketing and sale to eligible buyers. NOTE: Eligible buyers are typically U.S. Government organizations or U.S. Government contractors. Products approved for marketing and sale through the Authorized Vendor Program are placed on the Endorsed Cryptographic Products List. [G].
auto-manual system	Programmable, hand-held crypto-equipment used to perform encoding and decoding functions. [G].
automated security monitoring	Use of automated procedures to ensure security controls for an IS are not circumvented. [G].

automatic remote rekeying	Procedure to rekey a distant crypto- equipment electronically without specific actions by the receiving terminal operator. [G].
availability	The goal of ensuring that information and information processing resources both remain readily accessible to their authorized users. [J].
availability of data	Data that is in the place, at the time, and in the form needed by the user. [G].

B

backdoor	Synonymous with trap door. [G].
backup	Producing a copy of system files on separate media so that the system can be regenerated in the event of a crisis. [J].
bandwidth	A characteristic of a communications channel that is the amount of information that can be passed through it in a given amount of time, usually expressed in bits per second. [J].
baseline	<p>A set of critical observations or data used for a comparison or control.</p> <p>Note: Examples include a baseline security policy, a baseline set of security requirements, and a baseline system. [K].</p>
Bell-La Padula security model	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.) [G].
benign	<p>Condition of cryptographic data such that it cannot be compromised by human access to the data.</p> <p>NOTE: The term benign may be used to modify a variety of COMSEC-related terms, (e.g., key, data, storage, fill, and key distribution techniques). [G].</p>
benign environment	Non-hostile environment that may be protected from external hostile elements by physical, personnel, and procedural security countermeasures. [G].
beyond AI	<p>Level of trust employed by the DoD Trusted Computer System Evaluation Criteria that was beyond the state-of-the-art technology at the time the criteria was developed.</p> <p>NOTE: As defined in the "Orange Book," beyond AI includes all the AI-level features, plus others not required at the AI level. [G].</p>

BIBA integrity model	A model of integrity policy that describes restrictions on read and write based on integrity access classes of subjects and objects. A subject is allowed to write to an object only if the subject's integrity access class dominates the integrity class of the object. A subject is allowed to read from an object only if the subject's integrity access class is dominated by the object's integrity class. [J].
biometrics	Use of biological attributes (i.e., fingerprint, retina scan, voice print) to identify and authenticate a user to a system. [J].
binding	Process of associating a specific communications terminal with a specific cryptographic key or associating two related elements of information. [G].
bit error rate	Ratio between the number of bits incorrectly received and the total number of bits transmitted in a telecommunications system. [G].
BLACK	Designation applied to telecommunications and automated information systems, and to associated areas, circuits, components, and equipment, in which only unclassified signals are processed. NOTE: Encrypted signals are unclassified. [G].
BLACK key	Encrypted key. (See RED key.) [G].
breach	A failure or hole in a security mechanism or procedure that allows a violation of the system security policy. [J].
brevity list	List containing words and phrases used to shorten messages. [G].
browsing	Act of searching through IS storage to locate or acquire information, without necessarily knowing the existence or format of information being sought. [G].
bulk encryption	Simultaneous encryption of all channels of a multichannel telecommunications trunk. [G].
bypass	(1) To breach the security of a system by going around the protection features provided by the system. (2a) Message stream data not encrypted, typically protocol header information.(2b) The hardware/software implication of the mechanism which allows message

stream information to bypass the cryptographic element.
[J].

C

call back	Procedure for identifying a remote IS terminal, whereby the host system disconnects the caller and then dials the authorized telephone number of the remote terminal to re-establish the connection. [G].
call sign cipher	Cryptosystem used to encipher/decipher call signs, address groups, and address indicating groups. [G].
candidate TCB subset	The identification of the hardware, firmware, and software that make up the proposed TCB subset, along with the identification of its subjects and objects; one of the conditions for evaluation of parts. [J].
canister	Type of protective package used to contain and dispense key in punched or printed tape form. [G].
CAP	See Controlled Access Protection. [G]
capabilities	Where access to a protected object is granted if the requester possesses the appropriate "capability" that both identifies the object and specifies the access rights to be allowed to the user who possesses that capability. [H].
capability	Unforgeable ticket that provides incontestable proof that the presenter is authorized access to the object named in the ticket. [G].
capability-based system	IS in which access to protected objects is granted if the subject possesses a capability for the object. [G].
carve-out	A classified contract issued by a User Agency in connection with an approved Special Access Program in which DIS has been relieved of inspection responsibility in whole or in part. [J].
cascading problem	The cascading problem exists when a penetrator can take advantage of network connections to comprise information across a range of security levels that is greater than the accreditation range of any of the component systems he must defeat to do so. Cascading is possible in any connected network that processes a greater range of security levels than any one of its component system is accredited to handle. [J].

category	<p>Restrictive label that has been applied to both classified and unclassified data, thereby increasing the requirement for protection of, and restricting the access to, the data.</p> <p>NOTE: Examples include sensitive compartmented information, proprietary information, and North Atlantic Treaty Organization information. Individuals are granted access to special category information only after being granted formal access authorization. [G].</p>
caveats and handling restrictions	<p>Controls on the dissemination of information (e.g., For Official Use Only (FOUO), Privacy Act of 1974, Contract Sensitive, Company Propriety, NATO, and No Contractor). [I].</p>
CCI assembly	<p>Device embodying a cryptographic logic or other COMSEC design that the National Security Agency has approved as a controlled cryptographic item and performs the entire COMSEC function, but is dependent upon the host equipment to operate. [G].</p>
CCI component	<p>Device embodying a cryptographic logic or other COMSEC design, which the National Security Agency has approved as a controlled cryptographic item, that does not perform the entire COMSEC function and is dependent upon the host equipment or assembly to complete and operate the COMSEC function. [G].</p>
CCI equipment	<p>Telecommunications or information handling equipment that embodies a controlled cryptographic item component or controlled cryptographic item assembly and performs the entire COMSEC function without dependence on a host equipment to operate. [G].</p>
central office of record	<p>Office of a federal department or agency that keeps records of accountable COMSEC material held by elements subject to its oversight. [G].</p>
certificate of action statement	<p>Statement attached to a COMSEC audit report by which a COMSEC custodian certifies that all actions have been completed. [G].</p>
certification	<p>Comprehensive evaluation of the technical and nontechnical security features of an IS or component and other safeguards, made in support of the accreditation process, to establish the extent to which a particular design</p>

and implementation meets a set of specified security requirements. [G]. System certification should result in identifying residual risks as well as a recommendation to the Designated Approving Authority. [L].

certification agent

The individual(s) 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. [K].

Certification and Accreditation Plan

A plan delineating objectives, responsibilities, schedules, technical monitoring, and other activities in support of the C&A process. [K].

certification package

A product of the certification effort documenting the detailed results of the certification activities.

Note: The contents of this package will vary depending on the system. [K].

Certification Test and Evaluation (CT&E)

The software and hardware security tests conducted as part of the development. The purpose of these tests is to verify the security requirements have been correctly and completely implemented into the system. [M].

certified TEMPEST technical authority

U.S. Government or U.S. Government contractor employee designated to review the TEMPEST countermeasures programs of a federal department or agency. [G].

challenge and reply authentication

Prearranged procedure in which one communicator requests authentication of another and the latter establishes his/her validity with a correct reply. [G].

channel

An information transfer path within a system. May also refer to the mechanism by which the path is effected. [J].

checksum

Value computed, via some parity or hashing algorithm, on information requiring protection against error or manipulation. [G].

NOTE: Checksums are stored or transmitted with data and are intended to detect data integrity problems.

check word	Cipher text generated by a cryptographic logic to detect failures in the cryptography. [G].
cipher	Cryptographic system in which units of plain text are substituted according to a predetermined key. [G].
cipher text	Enciphered information. [G].
cipher text auto-key	Cryptographic logic which uses previous cipher text to generate a key stream. [G].
ciphony	Process of enciphering audio information, resulting in encrypted speech. [G].
Clark-Wilson integrity model	An integrity policy model with particular application to commercial transaction-oriented activities. The model describes controls on which transformations a user can invoke to access a given data item. [J].
Class C2	A set of criteria for evaluating the security features and level of assurance provided by a product, it does not specify or address how to implement the required security features to support system-specific information protection policies. "Class C2" applies to products ... both commercially-available products and custom-developed software, firmware and hardware products ... and the level of trust associated with their performance. [H].
classification	The determination that official information requires, in the interest of national security, a specific degree of protection against unauthorized disclosure, coupled with a designation signifying that such a determination has been made. Executive Order 12356 defines the following levels: Top Secret, Secret, Confidential, and Unclassified. [J].
classification authority	The authority that is vested in a government official to make an initial determination that information requires protection against unauthorized disclosure in the interest of national security. [J].
classification guide	A document issued by an authorized original classifier that prescribes the level of classification and appropriate declassification instructions for specific information to be classified on a derivative basis. (Classification guides are provided to contractors by the DD Form 254, "Department of Defense Contractor Security Classification Specification") [J].

classification information	National security information that has been classified pursuant to Executive Order 12356. [J].
classification management	The governing set of policies and procedures for identifying, controlling and protecting information, whether it is on a computer system or not. These policies apply not only to classified information but FOR OFFICIAL USE ONLY and Privacy Act information as well. [H].
classified contract	Any contract that requires or will require access to classified information by a contractor or his or her employees in the performance of the contract. A contract may be a classified contract even though the contract document is not classified... the requirements prescribed for a "classified contract" also are applicable to all phases of precontract activity, including solicitations (bids, quotations, and proposals), precontract negotiations, post-contract activity, or other projects which requires access to classified information contractors. [J].
classified information	National security information that has been classified pursuant to Executive Order 12356. [G].
clearance	An authorization allowing persons access to classified information. This is a "real-world" term used in connection with DoD policy, whose mathematical counterpart is a security level. A clearance typically consist of a level (Unclassified through Top Secret) and possibly one or more categories. See Category, Security level. [J].
clear text	Intelligible data, the semantic content of which is available. [J].
clearing	<p>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 normal system capabilities (i.e., through the keyboard).</p> <p>NOTE: An IS need not be disconnected from any external network before clearing takes place. Clearing enables a product to be reused within, but not outside of, a secure facility. It does not produce a declassified product by itself, but may be the first step in the declassification process. (See purge.) [G].</p>

closed security environment	<p>Environment that provides sufficient assurance that applications and equipment are protected against the introduction of malicious logic prior to or during the operation of a system.</p> <p>NOTE: Closed security is predicated upon a system's developers, operators, and maintenance personnel having sufficient clearances, authorization, and configuration control. [G].</p>
code	<p>System of communication in which arbitrary groups of letters, numbers, or symbols represent units of plain text of varying length.</p> <p>NOTE: Codes may or may not provide security. Common uses include: (a) converting information into a form suitable for communications or encryption, (b) reducing the length of time required to transmit information, (c) describing the instructions which control the operation of a computer, and (d) converting plain text to meaningless combinations of letters or numbers and vice versa. [G].</p>
code book	<p>Book or other document containing plain text and code equivalents in a systematic arrangement, or a technique of machine encryption using a word substitution technique. [G].</p>
code group	<p>Group of letters, numbers, or both in a code system used to represent a plain text word, phrase, or sentence. [G].</p>
code vocabulary	<p>Set of plain text words, numerals, phrases, or sentences for which code equivalents are assigned in a code system. [G].</p>
coercivity	<p>The strength of an applied magnetic field which will demagnetize a magnetic material. Demagnetizing the magnetic material of magnetic data storage media removes remanence. [I].</p>
cold start	<p>Procedure for initially keying crypto- equipment. [G].</p>
command authority	<p>Individual responsible for the appointment of user representatives for a department, agency, or organization and their key ordering privileges. [G].</p>
Commercial COMSEC	<p>Relationship between the National Security</p>

Endorsement Program	<p>Agency and industry, in which the National Security Agency 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.</p> <p>NOTE: Products developed under the Commercial COMSEC Endorsement Program may include modules, subsystems, equipment, systems, and ancillary devices. [G].</p>
Commercial Off The Shelf(COTS)	<p>COTS refer to those products that were commercially developed and are available for sale, rather than those that were specially developed for and funded by a specific customer(e.g., the U.S. Government). [J].</p>
common fill device	<p>One of a family of devices developed to read in, transfer, or store key.</p> <p>NOTE: KYK-13 Electronic Transfer Device, KYX-15 Net Control Device, and KOI-18 General Purpose Tape Reader are examples of common fill devices. [G].</p>
communications cover	<p>Concealing or altering of characteristic communications patterns to hide information that could be of value to an adversary. [G].</p>
communications deception	<p>Deliberate transmission, retransmission, or alteration of communications to mislead an adversary's interpretation of the communications. (See imitative communications deception and manipulative communications deception.) [G].</p>
communications field integrity	<p>The protection of any of the fields involved in network communications (e.g., protocol header, user data field) from unauthorized modification. [J].</p>
communications profile	<p>Analytic model of communications associated with an organization or activity.</p> <p>NOTE: The model is prepared from a systematic examination of communications content and patterns, the functions they reflect, and the communications security measures applied. [G].</p>
communications security	<p>Measures and controls taken to deny unauthorized persons information derived from telecommunications and ensure the authenticity of such telecommunications.</p>

NOTE: Communications security includes cryptosecurity, transmission security, emission security, and physical security of COMSEC material. [G].

comparable	Two security levels are comparable only if one dominates the other. If however, the first security level contains a category not in the second, and the second contains a category not in the first, then the two security levels are disjointed and not comparable. [J].
compartment	A class of information that has need-to-know controls based on formal access approval beyond those normally provided for access to Confidential, Secret or Top Secret information. [J].
compartmented 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 the most restricted information processed in the system. b. Formal access approval and signed non-disclosure agreements for that information to which a user is to have access. c. Valid need-to-know for information to which a user is to have access. [G].
Compartmented Mode Workstation (CMW)	A multilevel secure workstation product designed to meet requirements defined by the Defense Intelligence Agency's "Security Requirements for System High and Compartmented Mode Workstations," DRS-2600-5502-86. The CMW requirements fall between the B1 and B2 assurance classes described by the TCSEC with additional security requirements not addressed by the TCSEC, (e.g., advisory information labels). [J].
compartmented security mode	(A)IS security mode of operation wherein each user with direct or indirect access to 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 non-disclosure agreements for that information to which a user is to have access. (c) Valid

	need-to-know for information to which a user is to have access. [J].
component	A hardware, firmware, and/or software element or set of elements that perform a specific function and that may be used in a variety of operational environments.
compromise	Disclosure of information or data to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred. [G].
compromising emanations	Unintentional signals that, if intercepted and analyzed, would disclose the information transmitted, received, handled, or otherwise processed by telecommunications or automated information systems equipment. (See TEMPEST.) [G].
computer	The hardware, software, and firmware components of a system that are capable of performing calculations, manipulations, or storage of data. It usually consists of arithmetic, logical, and control units, and may have input, output, and storage devices. [K].
computer abuse	Intentional or reckless misuse, alteration, disruption, or destruction of data processing resources.
computer cryptography	Use of a crypto-algorithm program stored in software or firmware, by a general purpose computer to authenticate or encrypt/decrypt data for storage or transmission. [G].
computer security	<ol style="list-style-type: none">1. The protection resulting from all measures designed to prevent deliberate or inadvertent unauthorized disclosure, acquisition, manipulation, modification, or loss of information contained in a IS, as well as measures designed to prevent denial of authorized use of the system. [L].2. Addresses technical and procedural measures that can protect your computer system.
computer security incident	Any event in which a computer system is attacked, intruded into, or threatened with an attack or intrusion. [G].
computer security subsystem	Device designed to provide limited computer security features in a larger system environment. [G].

Computer Security Subsystem Interpretation (CSSI)	A document published by the NCSC interpreting the TCSEC for computer security subsystem. [J].
COMSEC account	Administrative entity, identified by an account number, used to maintain accountability, custody and control of COMSEC material. [G].
COMSEC account audit	Examination of the holdings, records, and procedures of a COMSEC account to ensure that all accountable COMSEC material is properly handled and safeguarded. [G].
COMSEC aid	COMSEC material, other than an equipment or device, that assists in securing telecommunications and which is required in the production, operation, or maintenance of COMSEC systems and their components. NOTE: COMSEC keying material, callsign/ frequency systems, and supporting documentation, such as operating and maintenance manuals, are examples of COMSEC aids. [G].
COMSEC boundary	Definable perimeter within a telecommunications equipment or system within which all hardware, firmware, and software components that perform critical COMSEC functions are located. NOTE: Key generation and key handling and storage are critical COMSEC functions. [G].
COMSEC chip set	Collection of National Security Agency approved microchips furnished to a manufacturer to secure or protect telecommunications equipment. (See secure communications and protected communications.) [G].
COMSEC control program	Set of instructions or routines for a computer that controls or affects the externally performed functions of key generation, key distribution, message encryption/decryption, or authentication. [G].
COMSEC custodian	Person designated by proper authority to be responsible for the receipt, transfer, accounting, safeguarding and destruction of COMSEC material assigned to a COMSEC account. NOTE: The term COMSEC manager is replacing the term COMSEC custodian. These terms are not synonymous,

since the responsibilities of the COMSEC manager extend beyond the functions required for effective operation of a COMSEC account. [G].

COMSEC end item

Equipment or combination of components ready for its intended use in a COMSEC application. [G].

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.

NOTE: COMSEC equipment includes crypto -equipment, crypto-ancillary equipment, crypto-production equipment, and authentication equipment. [G].

COMSEC facility

Space employed primarily for the purpose of generating, storing, repairing, or using COMSEC material. [G].

COMSEC incident

Occurrence that potentially jeopardizes the security of COMSEC material or the secure electrical transmission of national security information. [G].

COMSEC insecurity

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

COMSEC manager

Person who manages the COMSEC resources of a command or activity. (See the note following the definition for COMSEC custodian.) [G].

COMSEC material

Item designed to secure or authenticate telecommunications.

NOTE: 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. [G].

COMSEC Material Control System

Logistics and accounting system through which COMSEC material marked "CRYPTO" is distributed, controlled, and safeguarded.

NOTE: Included are the COMSEC central offices of record, crypto-logistic depots, and COMSEC accounts. COMSEC material other than key may be handled through the COMSEC Material Control System. [G].

COMSEC modification

Electrical, mechanical, or software change to a National Security Agency approved COMSEC end item.

NOTE: Categories of COMSEC modifications are: mandatory, optional, special mission mandatory, special mission optional, human safety mandatory, and repair actions. [G].

COMSEC module

Removable component that performs COMSEC functions in a telecommunications equipment or system. [G].

COMSEC monitoring

Act of listening to, copying, or recording transmissions of one's own official telecommunications to provide material for analysis, so that the degree of security being provided to those transmissions may be determined. [G].

COMSEC profile

Statement of the COMSEC measures and materials used to protect a given operation, system, or organization. [G].

COMSEC survey

Organized collection of COMSEC and communications data relative to a given operation, system, or organization. [G].

COMSEC system data

Information required by a COMSEC equipment or system to enable it to properly handle and control key. [G].

COMSEC training

Teaching of hands-on skills relating to COMSEC accounting, the use of COMSEC aids, or the installation, use, maintenance, and repair of COMSEC equipment. [G].

Confidential (C)

"CONFIDENTIAL" is the designation that shall be applied to information or material the unauthorized disclosure of which could be reasonably expected to cause damage to the national security. Example of "damage" include the comprise of information that indicates strength of ground, air, and naval forces in the U.S. and overseas areas; disclosure of technical information used for training, maintenance, and inspection of classified munitions of war; and revelation of performance characteristics, test data, design, and production data on munitions of war. [J].

confidentiality	<ol style="list-style-type: none">1. Assurance that information is not disclosed to unauthorized entities or processes. [G].2. The concept of holding sensitive data in confidence, limited to an appropriate set of individuals or organizations.
configuration	Selection of one of the set of possible combinations of features of a systems. [J].
configuration control	Process of controlling modifications to a telecommunications or automated information systems hardware, firmware, software, and documentation to ensure the system is protected against improper modifications prior to, during, and after system implementation. [G].
configuration management	Management of security features and assurances through control of changes made to hardware, software, firmware, documentation, test, test fixtures and test documentation of an automated information system, throughout the development and operational life of a system. [G].
confinement	The prevention of the leaking of sensitive data from a program. [J].
confinement channel	See covert channel. [J].
confinement property	Synonymous with star (*) property. [G].
contamination	The intermixing of data at different sensitivity and need-to-know levels. The lower level data is said to be contaminated by the higher level data; thus, the contaminating (higher level) data may not receive the required level of protection. [J].
content dependent access control	Access control in which access is determined by the value of the data to be accessed. [J].
context dependent access control	Access control in which access is determined by the specific circumstances under which the data is being accessed. [J].

contingency key	Key held for use under specific operational conditions or in support of specific contingency plans. [G].
contingency plan	Plan maintained for emergency response, backup operations, and post-disaster recovery for an IS, as a part of its security program, that will ensure the availability of critical resources and facilitate the continuity of operations in an emergency situation. [G].
continuity of operations	The maintenance of operations availability through resistance to denial-of-service attacks. This may be accomplished by providing redundant components, fault tolerant systems, degraded or priority service, and automatic service adaptation. This may be required for systems supporting critical functions or missions. [J].
control objective	Required result of protecting information within an IT product and its immediate environment. [J].
control zone	The space, expressed in feet of radius, surrounding equipment processing sensitive information, that is under sufficient physical and technical control to preclude unauthorized entry or compromise. [J].
Controlled Access Protection	<p>1. Log-in procedures, audit of security relevant events, and resource isolation as prescribed for class C2 in the Orange Book. [G].</p> <p>2. A term which describes the minimum set of automated controls that should be provided to ISs (i.e., discretionary access control (DAC), user identification and authentication (I&A), auditing of security-relevant events, and clearing of memory and storage before reuse.</p>
controlled cryptographic item	<p>Secure telecommunications or information handling equipment, or associated cryptographic component, that is unclassified but governed by a special set of control requirements.</p> <p>NOTE: Such items are marked "CONTROLLED CRYPTOGRAPHIC ITEM" or, where space is limited, "CCI." [G].</p>
Controlled Security Mode	An IS is operating in controlled mode, a reduced form of multilevel mode, when a more limited degree of trust is placed in the IS and the classification and clearance levels are restricted. [H].

controlled sharing	Condition which exists when access control is applied to all users and components of an IS. [G].
controlled space	Three-dimensional space surrounding telecommunications and automated information systems equipment, within which unauthorized persons are denied unrestricted access and are either escorted by authorized persons or are under continuous physical or electronic surveillance. [G].
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. [G].
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. [G].
cooperative remote rekeying	Synonymous with manual remote rekeying. [G].
correctness	The extent to which a program satisfies its specifications. [J].
cost-benefit analysis	Assessment of the costs of providing protection or security to a telecommunications or IS versus risk and cost associated with asset loss or damage. [G].
cost-risk analysis	The assessment of the costs of providing data protection for a system versus the cost of losing or compromising the data. [J].
countermeasure	Action, device, procedure, technique, or other measure that reduces the vulnerability of an IS. [G].
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.) [G].
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 channel analysis properly includes all forms of cover

channels, external as well as internal, and timing as well as storage channels. [J].

covert storage/data channel

Covert channel that involves 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.

NOTE: Covert storage channels typically involve a finite resource (e.g., sectors on a disk) that is shared by two subjects at different security levels. [G].

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. [G].

credentials

Information, passed from one entity to another, that is used to establish the sending entity's access rights. [G].

criteria

See Trusted Computer System Evaluation Criteria. [J].

criteria interpretation

Interpretations of the TCSEC where additional specificity was needed. These criteria interpretations are located on Dockmaster (an NSA computer system) on the "Announce" forum. In addition, interpretations for specific application areas such as subsystems (CSSI), networks(TNI), and databases(TDI) were developed and each published in a separate document available from the NSA. [J].

critical nuclear weapon design information

TOP SECRET RESTRICTED DATA or SECRET design information RESTRICTED DATA revealing the theory of operation or design of the components of a thermo-nuclear or implosion-type fission bomb, warhead, demolition munitions, or test device. Specifically excluded is information concerning arming, fusing, and firing systems; limited life components; and totally contained quantities of fissionable, and high explosive materials by type. Among these excluded items are components which DoD personnel, including contractor personnel, set, maintain, operate, test, or replace. [J].

criticality	A measure of how important the correct and uninterrupted functioning of the system is to national security, human life or safety, or the mission of the using organization. [J].
cryptanalysis	Operations performed in converting encrypted messages to plain text without initial knowledge of the crypto-algorithm and/or key employed in the encryption. [G].
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. NOTE: When written in all upper case letters, CRYPTO has the meaning stated above. When written in lower case as a prefix, crypto and crypt are abbreviations for cryptographic. [G].
crypto-alarm	Circuit or device which detects failures or aberrations in the logic or operation of crypto-equipment. NOTE: Crypto-alarm may inhibit transmission or may provide a visible and/or audible alarm. [G].
crypto-algorithm	Well-defined procedure or sequence of rules or steps used to produce cipher text from plain text and vice versa. [G].
crypto-ancillary equipment	Equipment designed specifically to facilitate efficient or reliable operation of crypto-equipment, but that does not perform cryptographic functions. [G].
crypto-equipment	Equipment that embodies a cryptographic logic. [G].
cryptographic	Pertaining to, or concerned with, cryptography. [G].
cryptographic checksum	A checksum that is generated using cryptographic means. It is used to detect accidental or deliberate modification of data. See message authentication code. [J].
cryptographic component	Hardware or firmware embodiment of the cryptographic logic. NOTE: Cryptographic component may be a modular assembly, a printed wiring assembly, a microcircuit, or a combination of these items. [G].

cryptographic initialization	Function used to set the state of a cryptographic logic prior to key generation, encryption, or other operating mode. [G].
cryptographic key	A bit pattern used to determine specific characteristics of the encryption/decryption algorithm (e.g., the specific substitutions and permutations to be made in the plaintext and intermediate results) in order to encrypt/decrypt the message. Cipher systems are usually designed so that it is very hard to decipher cipher text without knowledge of the cryptographic key. [J].
cryptographic logic	Well-defined procedure or sequence of rules or steps used to produce cipher text from plain text, and vice versa, or to produce a key stream, plus delays, alarms, and checks which are essential to effective performance of the cryptographic process. (See crypto algorithm.) [G].
cryptographic randomization	Function which randomly determines the transmit state of a cryptographic logic. [G].
cryptography	Principles, means, and methods for rendering plain information unintelligible and for restoring encrypted information to intelligible form. [G].
crypto-ignition key	Device or electronic key used to unlock the secure mode of crypto-equipment. [G].
cryptonet	Stations that hold a specific key for use. NOTE: Activities that hold key for other than use, such as crypto-logistic depots, are not cryptonet members for that key. Controlling authorities are defacto members of the cryptonets they control. [G].
cryptoperiod	Time span during which each key setting remains in effect. [G].
cryptosecurity	Component of communications security that results from the provision of technically sound cryptosystems and their proper use. [G].
cryptosynchronization	Process by which a receiving decrypting cryptographic logic attains the same internal state as the transmitting encrypting logic. [G].
cryptosystem	Associated COMSEC items interacting to provide a single means of encryption or decryption. [G].

cryptosystem assessment	Process of establishing the exploitability of a cryptosystem, normally by reviewing transmitted traffic protected or secured by the system under study. [G].
cryptosystem evaluation	Process of determining vulnerabilities of a cryptosystem. [G].
cryptosystem review	Examination of a cryptosystem by the controlling Authority to ensure its adequacy of design and content, continued need, and proper distribution. [G].
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. [G].

D

data	Information with a specific physical representation. [J].
data encryption standard	Cryptographic algorithm, designed for the protection of unclassified data and published by the National Institute of Standards and Technology in Federal Information Processing Standard Publication 46. [G].
data flow control	Synonymous with information flow control. [G].
data integrity	Condition that exists when data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed. [G].
data origin authentication	Corroboration that the source of data is as claimed. [G].
data security	Protection of data from unauthorized (accidental or intentional) modification, destruction, or disclosure. [G].
Database Management System (DBMS)	A computer system whose main function is to facilitate the sharing of a common set of data among many different users. It may or may not maintain semantic relationships among the data items. [J].
decertification	Revocation of the certification of an IS item or equipment for cause. [G].
declassification	The determination that classified information no longer requires, in the interest of national security, any degree of protection against unauthorized disclosure, coupled with a removal or cancellation of the classification designation. Declassification does not constitute authority for public release. Declassification may be accomplished only under the rules contained in OPNAVINST 5510.1. [I].
decipher	Convert enciphered text to the equivalent plain text by means of a cipher system. [G].
decode	Convert encoded text to its equivalent plain text by means of a code. [G].
decrypt	Generic term encompassing decode and decipher. [G].

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 non-disclosure agreements for all the information stored and/or processed (including all compartments, subcompartments, and/or special access programs).
- c. Valid need-to-know for all information contained within the IS.

NOTE: 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. [G].

Dedicated (Security) Mode

An IS is operating in the dedicated mode when all of its users possess the proper security clearance and have need-to-know for accessing all data processed and stored by the IS. ISs containing only unclassified information, as well as those containing both unclassified and classified information, can operate in the dedicated mode. All information is handled at the highest classification processed by the system. [H].

default classification

Temporary classification reflecting the highest classification being processed in an IS.

NOTE: Default classification is included in the caution statement affixed to the object. [G].

degauss

Destroy information contained in magnetic media by subjecting that media to high intensity alternating magnetic fields, following which the magnetic fields slowly decrease. [G].

degausser

An electrical device (AC or DC) or a hand-held magnet assembly which can generate coercive magnetic force for the purpose of degaussing magnetic storage media or other magnetic material. [J].

Degausser Product List (DPL)	A list of commercially produced degaussers that have been evaluated against specific requirements for the erasure of classified data from magnetic media. This list is included in the Information Systems Security Products and Service Catalogue Supplement; Oct. 93.
delegated development program	Information systems security program in which the Director, National Security Agency, delegates the development and/or production of the entire telecommunications product, including the information systems security portion, to a lead department or agency. [G].
denial of service	Result of any action or series of actions that prevents any part of a telecommunications or IS from functioning. [G].
descriptive top-level specification	Top-level specification that is written in a natural language (e.g., English), an informal design notation, or a combination of the two. NOTE: Descriptive top-level specification, required for a class B2 and B3 IS, completely and accurately describes a trusted computing base. (See formal top-level specification.) [G].
Design Analysis Phase (DAP)	The third phase of the NSA evaluation process where an in-depth analysis of the design of the system is performed in order to ensure that the design meets all the TCSEC requirements at its evaluation class. The evaluation team looks at all the supplied design documentation to perform this analysis. Their analysis is presented to a technical review board for review and comment. [J].
design controlled spare part	Part or subassembly for a COMSEC equipment or device with a National Security Agency controlled design. [G].
Designated Approving Authority	<ol style="list-style-type: none">1. Official with the authority to formally assume responsibility for operating an IS or network at an acceptable level of risk. [G].2. Responsible for the following: issuing an accreditation statement that records the decision to accept all security risks and countermeasures; determining the acceptable level of data remanence risk for each system that will be accredited; approving software programs and equipment used for clearing and purging data storage media, and

	approving procedures for removal of external markings from data storage media. Only those persons having DAA cognizance over a particular system or medium have authority to approve purging or clearing procedures.
designated countries	Those countries whose policies are inimical to U.S. interest. Travel to designated countries by cleared personnel must be reported to the security manager prior to trip initiation.
development assurance component	Fundamental building block, specifying how an IT product is developed, from which development assurance requirements are assembled. [J].
development assurance requirements	Requirements in a protection profile which address how each conforming IT product is developed including the production of appropriate supporting developmental process evidence and how that product will be maintained. [J].
device labels	Labels that constrain the range (sensitivity) of data that can be stored or processed on the device. [J].
dial back	Synonymous with call back. [G].
digital signature	Synonymous with electronic signature. [G].
direct shipment	Shipment of COMSEC material directly from the National Security Agency to user COMSEC accounts. [G].
disclosure	information exposure to someone without appropriate clearance and/or authorization. [J].
Discretionary Access Control	Means of restricting access to objects based on the identity and need-to-know of users and/or groups to which the object belongs. NOTE: 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.) [G].
discretionary security property	A Bell-LaPadula security model rule which requires that all current accesses be allowed by the access control matrix. [J].

disjoint	In comparing two security levels S1 and S2, when neither security level dominates the other they are said to be disjointed. This occurs when S1 includes non-hierarchical categories not present in S2 and S2 includes non-hierarchical categories not present in S1. [J].
dockmaster	A B2 Multics machine run by the NSA. It is used by the NSA and the security community to communicate and exchange ideas. Dockmaster supports a number of "forums" that are used to discuss issues related to computer security. In addition, Dockmaster is used heavily by the NSA evaluation teams and vendor community to discuss ongoing evaluations. For more information on Dockmaster call (800) 336-3625 or (410) 850-4446 within Maryland. [J].
DoD component	Refers to the Office of the Secretary of Defense (OSD), the Military Departments and services within those departments, the Chairman of the Joint Chiefs of Staff and the Joint Staff, the unified and specified commands, the defense agencies, and the DoD field activities. [K].
DoD Trusted Computer System Evaluation Criteria	Document containing basic requirements and evaluation classes for assessing degrees of effectiveness of hardware and software security controls built into IS. NOTE: This document, DoD 5200.28 STD, is frequently referred to as the Orange Book. [G].
domain	Unique context (e.g. , access control parameters) in which a program is operating; in effect, the set of objects that a subject has the ability to access. [G].
dominate	Term used to compare IS security levels. NOTE: Security level S ₁ is said to dominate security level S ₂ if the hierarchical classification of S ₁ is greater than, or equal to, that of S ₂ and the non-hierarchical categories of S ₁ include all those of S ₂ as a subset. [G].
downgrade	This is a determination that classified information requires, in the interest of national security, a lower degree of protection against unauthorized disclosure than currently provided, together with a changing of the classification designation to reflect such a lower degree of protection. [J].

downgrader	A human or a automated information system that has the privilege and authority to downgrade information. [J].
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. NOTE: Local accountability of the COMSEC material may continue to be required. (See accounting legend code, ALC-3 and ALC-4.) [G].
dual control	The process of utilizing two or more separate entities (usually persons) operating in concert, to protect sensitive functions or information. Both (all) entities are equally responsible. This approach generally involves the split knowledge [of the] physical or logical protection of security parameters. [J].
dummy group	Textual group having the appearance of a valid code or cipher group which has no plain text significance. [G].

E

electronically generated key	<p>Key produced only in non-physical form. [G].</p> <p>NOTE: Electronically generated key stored magnetically (e.g., on a floppy disc) is not considered hard copy key. [G].</p>
electronic signature	<p>Process that operates on a message to assure message source authenticity and integrity, and source non-repudiation. [G].</p>
electronic security	<p>Protection resulting from all measures designed to deny unauthorized persons information of value which might be derived from the interception and analysis of non-communications electromagnetic radiations, such as radar. [G].</p>
element	<p>Removable item of COMSEC equipment, assembly, or subassembly which normally consists of a single piece or group of replaceable parts. [G].</p>
emanation security	<p>The protection resulting from all measures taken to deny unauthorized persons information of value that might be derived from the interception and from an analysis of compromising emanations from systems. See TEMPEST. [J].</p>
emanations	<p>See compromising emanations. [J].</p>
embedded computer	<p>Computer system that is an integral part of a larger system or subsystem that performs or controls a function, either in whole or in part. [G].</p>
embedded cryptography	<p>Cryptography which is engineered into an equipment or system the basic function of which is not cryptographic.</p> <p>NOTE: Components comprising the cryptographic module are inside the equipment or system and share host device power and housing. The cryptographic function may be dispersed or identifiable as a separate module within the host. [G].</p>

embedded cryptographic system	Cryptosystem that performs or controls a function, either in whole or in part, as an integral element of a larger system or subsystem. [G].
emission security	Protection resulting from all measures taken to deny unauthorized persons information of value which might be derived from intercept and analysis of compromising emanations from crypto- equipment, IS, and telecommunications systems. [G].
encapsulated object	A data structure whose existence is known, but whose internal organization is not accessible, except by invoking the encapsulated subsystem that manages it. [J].
encapsulated subsystem	A collection of procedures and data objects that is protected in a domain of its own so that the internal structure of a data object is accessible only to the procedures of the encapsulated subsystem and that the procedures may be called only at designated domain entry points. Encapsulated subsystems, protected subsystem, and protected mechanism of the TCB are terms that may be used interchangeably. [J].
encipher	Convert plain text to equivalent cipher text by means of a cipher. [G].
encode	Convert plain text to equivalent cipher text by means of a code. [G].
encrypt	Generic term encompassing encipher and encode. [G].
encryption	Using cryptographic means to render information unintelligible in a manner that allows the information to be decrypted into its original form. The process of transforming plaintext into ciphertext. [J].
end-item accounting	Accounting for all the accountable components of a COMSEC equipment configuration by a single short title. [G].
Endorsed Cryptographic Product List	A list of products that provide electronic cryptographics coding (encrypting) and decoding (decrypting), and which have been endorsed for use for classified or sensitive unclassified U.S. Government or Government-driven information during its transmission. It is included in the INFOSEC Catalogue. [L].

endorsed DES equipment	Unclassified equipment that embodies unclassified data encryption standard cryptographic logic and has been endorsed by the National Security Agency for the protection of national security information. [G].
Endorsed Tools List (ETL)	The list of formal verification tools endorsed by the NCSC for the development of systems with high levels of trust. [J].
endorsed for unclassified cryptographic item	Unclassified cryptographic equipment that embodies a U.S. Government classified cryptographic logic and is endorsed by the National Security Agency for the protection of national security information. (See type 2 product.) [G].
endorsement	National Security Agency approval of a commercially developed telecommunications or automated information systems protection equipment or system for safeguarding national security information. [G].
end-to-end encryption	Encryption of information at its origin, and decryption at its intended destination, without any intermediate decryption. [G].
end-to-end security	Safeguarding information in a secure telecommunications system by cryptographic or protected distribution system means from point-of-origin to point-of-destination. [G].
Enhanced Hierarchical Development Methodology (EHDM)	An integrated set of tools designed to aid in creating, analyzing, modifying, managing, and documenting program specifications and proofs. This methodology includes a specification parser and typechecker, a theorem prover, and multi-level security checker. [J].
entrapment	Deliberate planting of apparent flaws in an IS for the purpose of detecting attempted penetrations. [G].
environment	Procedures, conditions, and objects that affect the development, operation, and maintenance of an IS. [G].
erasing	Ambiguous term which can refer to purging, clearing, or removing file allocation. [I].
erasure	Process intended to render stored data irretrievable by normal means. [G].

Evaluated Products List (EPL)	A documented inventory of equipment, hardware, software, and/or firmware that have been evaluated against the evaluation criteria found in DoD 5200.28-STD. The EPL is included in the Information Systems Security Products and Service Catalogue Supplement; Oct. 93.
evaluation	The technical assessment of a component's, subsystem's, or system's security that establishes whether or not the component, subsystem, or system meets a specific set of requirements. In the security community two types of evaluation are commonly used: (1) evaluations that exclude the application environment, and (2) evaluations that include the application environment. This second type of evaluation, meaning an evaluation conducted to assess a system's security attributes with respect to a specific operational mission, is what is referred to as "certification." Evaluations that exclude the application environment are assessments of the security countermeasures against a standard/criteria. The term "evaluation" refers to a security assessment of a <u>product</u> against a given set of criteria/standards, while "certification" refers to a security assessment of a <u>system</u> or operating environment against a given set of security requirements. [L].
evaluation assurance component	Fundamental building block, specifying the type and the rigor of required evaluation activities, from which evaluation assurance requirements are assembled. [J].
evaluation assurance requirements	Requirements in a protection profile which address both the type and the rigor of activities that must occur during product evaluation. [J].
evaluator	One who performs the security evaluation. For example, a member of an NSA security evaluation team. These individuals usually come from organizations such as NSA, The Aerospace Corporation, and The MITRE Corporation. [J].
exception	With respect to C&A, an exception indicates the implementation of one or more security requirements is temporarily postponed and that satisfactory substitutes for the requirements may be used for a specified period of time. (see Waiver) [K].

executive state	<p>One of several states in which an IS may operate, and the only one in which certain privileged instructions may be executed.</p> <p>NOTE: Such privileged instructions cannot be executed when the system is operating in other (e.g., user) states. [G].</p>
exercise key	<p>Key intended to safeguard transmissions associated with exercises. [G].</p>
exploitable channel	<p>Covert channel that is intended to violate the security policy governing an IS and is useable or detectable by subjects external to the trusted computing base. (See covert channel.) [G].</p>
exploratory development model	<p>Assembly of preliminary circuits or parts in line with commercial practice to investigate, test, or evaluate the soundness of a concept, device, circuit, equipment, or system in a "breadboard" or rough experimental form, without regard to eventual overall physical form or layout. [G].</p>
extraction resistance	<p>Capability of a crypto-equipment or a secure telecommunications system or equipment to resist efforts to extract key. [G].</p>

F

facility (security) clearance	An administrative determination that, from a security viewpoint, a facility is eligible for access to classified information of a certain category (and all lower categories). [J].
fail safe	Pertaining to the automatic protection of programs and/or processing systems to maintain safety when a hardware or software failure is detected in a system. [G].
fail soft	Pertaining to the selective termination of affected nonessential processing when a hardware or software failure is determined to be imminent in an IS. [G].
failure access	Unauthorized and usually inadvertent access to data resulting from a hardware or software failure in an IS. [G].
failure control	Methodology used to detect and provide fail safe or fail soft recovery from hardware and software failures in an IS. [G].
fault	a condition that causes a device or system component to fail to perform in a required manner. [J].
fetch protection	IS-provided restriction to prevent a program from accessing data in another users segment of storage. [G].
fielded equipment	COMSEC end-item shipped to the user subsequent to first article testing on the initial production contract. [G].
file protection	Aggregate of all processes and procedures established in an IS designed to inhibit unauthorized access, contaminations elimination, modification, or destruction of a file or any of its contents. [G].
file security	Means by which access to computer files is limited to authorized users only. [G].
fill device	COMSEC item used to transfer or store key in electronic form or to insert key into a crypto-equipment. [G].
Final Evaluation Report (FER)	The final report generated by the NSA that documents the results of the completed evaluation of a trusted product by the NSA. The FER documents the TCSEC rating achieved

by the product, provides an overview of the security features of the product, describes how it meets the requirements of its evaluation class, and lists its evaluated configuration. [J].

FIREFLY	Key management protocol based on public key cryptography. [G].
firmware	Equipments or devices within which computer programming instructions necessary to the performance of the device's discrete functions are electrically embedded in such a manner that they cannot be electrically altered during normal device operations.
Firewall	Used to control access to or from a protected network. Enforces a network access policy by forcing connections to pass through this system, where they can be examined and evaluated. The system can be a router, a personal computer, a host, or a collection of hosts, set up specifically to shield a site or subnet from protocols and services that can be abused from hosts outside the subnets. [O].
fixed COMSEC facility	COMSEC facility that is located in an immobile structure or aboard a ship. [G].
flaw	Error of commission, omission, or oversight in an IS that may allow protection mechanisms to be bypassed. [G].
flaw hypothesis methodology	System analysis and penetration technique in which the specification and documentation for an IS are analyzed and then flaws in the system are hypothesized. NOTE: List of hypothesized flaws is prioritized on the basis of the estimated probability that a flaw exists and, assuming a flaw does exist, 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. [G].
flow analysis	See Information Flow Analysis. [J].
flow control	See Information Flow Control. [J].
For Official Use Only (FOUO)	Information that has not been given a security classification pursuant to the criteria of an Executive Order, but which may be withheld from public disclosure

under the criteria of the Freedom of Information Act, Title 5, U.S.C., Section 552. [J].

Foreign Ownership, Control
or Influence (FOCI)

FOCI refers to the foreign ownership, control or influence of a company involved in work that can affect national security. [J].

formal access approval

Documented approval by a data owner to allow access to a particular category of information. [G].

Formal Development Methodology
(FDM)

A collection of languages and tools that enforces a rigorous method of verification. This methodology uses the Ida Jo specification language for successive stages of system development, including identification and modeling of requirements, high-level design, and program design. This methodology is on the NSA Endorsed Tool List (ETL). [J].

formal evaluation phase

The fourth phase of the NSA evaluation process where the finalized and marketable product is frozen and then hands-on testing is performed by the evaluation team. The results of these tests are presented to the Technical Review Board. Upon completion of this phase a product receives its formal rating and is placed on the Evaluation Product List (EPL). [J].

formal proof

Complete and convincing mathematical argument, presenting the full logical justification for each proof step, for the truth of a theorem or set of theorems.

NOTE: In computer security, these formal proofs provide AI, and beyond AI assurance under the DoD Trusted Computer System Evaluation Criteria. [G].

formal security policy model

Mathematically precise statement of a security policy.

NOTE: 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 that the initial state is secure and that all possible subsequent states remain secure. [G].

formal specification

A specification of hardware or software in a computer-readable language, usually giving a precise mathematical description of the behavior of the system with the intention of providing support for formal verification. Formal specification for a system can be written at any

level of detail. See Top Level Specification and Formal Top Level Specification. [J].

formal top-level specification

Top-level specification that is 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.

NOTE: Formal top-level specification, required for a class A1 IS, completely and accurately describes the trusted computing base. (See descriptive top level specification.) [G].

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). [G].

formally restricted data

Information removed from the RESTRICTED DATA category upon a joint determination by the DOE (or antecedent agencies) and the DOD that such information relates primarily to the military utilization of atomic weapons, and that such information can be adequately safeguarded as classified defense information. For purposes of foreign dissemination, however, such information is treated in the same manner as RESTRICTED DATA. [J].

frequency hopping

Repeated switching of frequencies during radio transmission according to a specified algorithm, to minimize unauthorized interception or jamming of telecommunications. [G].

front-end security filter

Security filter, which could be implemented in hardware or software, that is logically separated from the remainder of an IS to protect the integrity of the system. [G].

full maintenance

Complete diagnostic repair, modification, and overhaul of information systems security equipment, including repair of defective assemblies by piece part replacement. (See limited maintenance.) [G].

functional component

Fundamental building block., specifying what an IT product must be capable of doing, from which functional protection requirements are assembled. [J].

functional protection requirements	Requirements in a protection profile which address what conforming IT products must be capable of doing. [J].
functional testing	Segment of security testing in which advertised security mechanisms of an IS are tested under operational conditions. [G].
future change review board	The panel who reviews future evaluated product changes and makes a recommendation to the NSA on the composition of the Security Analysis Team (SA-Team). The FCRB consists of Technical Review Board (TRB) members and other personnel as appointed by the NSA. The FCRB recommends the composition of the SA-Team and the mode of presentation by the SA-Team to the RAMP TRB. [J].

G

global requirements	Those which require analysis of the entire system and for which separate analysis of the individual TCB subsets does not suffice. [J].
granularity	Relative fineness or coarseness to which an access control mechanism can be adjusted. NOTE: Protection at the file level is considered coarse granularity, whereas protection at the field level is considered to be a finer granularity. [G].
greatest lower bound	In comparing two security levels S1 and S2, the unique security level that is dominated by S1 and S2 and dominates all other security levels that are dominated by both S1 and S2. See least upper bound. [J].
group accreditation	Accreditation of a group of systems having a common security policy and similar residual risks.
guard	Processor that provides a filter between two disparate systems operating at different security levels or between a user terminal and a data base to remove data for which the user is not authorized access. [G].
gypsy verification environment	An integrated set of tools for specifying, coding, and verifying programs written in the Gypsy language, a language similar to Pascal which has both specification and programming features. This methodology includes an editor, a specification processor, a verification condition generator, a user-directed theorem prover, and an information flow tool. This methodology is currently on the NSA's Endorsed Tools List (ETL) for verification tools. [J].

H

handshaking procedures	Dialogue between two entities (e.g., a user and a computer, a computer and another computer, or a program and another program) for the purpose of identifying and authenticating these entities to one another. [G].
hard copy key	Physical keying material, such as printed key lists, punched or printed key tapes, or programmable, read-only memories. [G].
hardware	The electric, electronic, and mechanical equipment used for processing data.
hardwired key	Key that is permanently installed. [G].
hashing	Iterative process that computes a value (referred to as a hashword) from a particular data unit in a manner that, when a hashword is protected, manipulation of the data is detectable. [G].
hashword	Synonymous with checksum. [G].
Hierarchical Development Methodology (HDM)	A methodology for specifying and verifying design [specifications] written in the Special specification language. The tools for this methodology include the Special specification processor, the Boyer-Moore theorem prover, and the Feiertag information flow tool. [J].
hierarchical level	In Mandatory Access Control, hierarchical refers to the security level portion of a clearance or classification where each allowed value is either greater than or less than each other value, thus forming a complete ordering from highest to lowest(e.g., Unclassified < Confidential < Secret < Top Secret). Contrast Non-Hierarchical categories or special access requirements where each value is independent of every other value. See Domains and Non-Hierarchical Category. [J].
high risk environment	Specific location or geographic area where there are insufficient friendly security forces to ensure the safeguarding of information systems security equipment. [G].

high-water mark	Of two or more security levels, the highest of the hierarchical classifications, and the set union of the non-hierarchical categories. [J].
hostile cognizant agent	Person, authorized access to national security information, who intentionally makes that information available to an intelligence service or other group, the goals of which are inimical to the interests of the United States Government or its allies. [G].
host to front-end protocol	Set of conventions governing the format and control of data that is passed from a host to a front-end machine. [G].
hot key	A Secure Attention Key. See also Attention Character. [J].

I

identification	Process that enables recognition of an entity by an IS. [G].
Identification & Authentication (I&A)	<p>The process that enables an (A)IS to recognize an entity and verify the entity's identity. [J].</p> <p>NOTE: This is generally accomplished by the use of unique machine-readable user names. [G].</p>
imitative communications deception	Introduction of deceptive messages or signals into an adversary's telecommunications signals. (See communications deception and manipulative communications deception.) [G].
impersonation	Synonymous with spoofing. [G].
implant	Electronic device or component modification to electronic equipment that is designed to gain unauthorized interception of information-bearing energy via technical means. [G].
implementation	The phase of the system development process in which the detailed specifications are translated into actual system components. [K].
IDA JO	A nonprocedural state-transition specification language used in Unisys Corporation's specification and verification methodology. [J].
inadvertent disclosure	Accidental exposure of information to a person not authorized access. [G].
incomplete parameter checking	IS design flaw that results when all parameters have not been fully anticipated for accuracy and consistency, thus making the system vulnerable to penetration. [G].
individual accountability	Ability to associate positively the identity of a user with the time, method, and degree of access to an IS. [G].
industrial security	That portion of information security which is concerned with the protection of classified information in the hands of U.S. industry. [J].

inference	Refer to the deduction of information for which a user is not authorized from information to which the user is authorized. [J].
inference control	In databases, the procedures, processes and controls in effect which limits inference. [J].
Informal Security Policy Model (ISPM)	An informal (e.g., English) representation of a security policy model. See security policy model. [J].
information flow analysis	Tracing the flow of specific information types through an information system to determine whether control applied to this information are appropriate. [J].
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. [G].
information label	<p>Piece of information that accurately and completely represents the sensitivity of the data in a subject or object.</p> <p>NOTE: Information label consists of a security label as well as other required security markings (e.g., codewords, dissemination control markings, and handling caveats), to be used for data information security labeling purposes. [G].</p>
information security	The result of any system of policies and procedures for identifying, controlling, and protecting, from unauthorized disclosure, information whose protection is authorized by Executive Order or statute. [J].
information sensitivity	Sensitivity of unclassified information shall be determined in accordance with applicable information protection policies regarding information sensitivity and requirements for its control. Sensitivity shall also be considered with respect to unauthorized disclosure and/or modification. The effect of data aggregation and inference shall be considered when determining the sensitivity of information. Some elements, when considered separately, may each be of relatively low sensitivity; however, when considered collectively, these same elements become significantly more sensitive to unauthorized disclosure. [H].
Information System	Any telecommunications and/or computer related equipment or interconnected system or subsystems of equipment that is used in the acquisition, storage,

manipulation, management, movement, control, display, switching, interchange, transmission, or reception of voice and/or data, and includes software, firmware, and hardware. [G].

information systems security
(INFOSEC)

The protection of ISs against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats. [G]. IS security includes consideration of all hardware and/or software functions, characteristics, and/or features; operational procedures, accountability procedures, and access controls at the central computer facility, remote computer, and terminal facilities; management constraints; physical structures and devices; and personnel and communications controls needed to provide an acceptable level of risk for the IS and for the data and information contained in the IS.

Information System Security
Manager (ISSM)

Person responsible to the activity's DAA who develops, maintains, and directs the implementation of the INFOSEC program within the activity. The ISSM advises the CO on all INFOSEC matters, including identifying the need for additional INFOSEC staff. Serves as the Command's point of contact for all INFOSEC matters and implements the command's INFOSEC program. Previously the ADP Security Officer.

Information System Security
Officer (ISSO)

Person responsible for ensuring that security is provided for and implemented throughout the life cycle of an information resource. Responsible for implementing system specific security policies in the operational environment. ISSO's are typically responsible for single-user computers (e.g., personal computers and workstations), multi-user computers or departmental Local Area Networks (LANs). The ISSO assists the ISSM in implementing the command's INFOSEC program for an assigned system or area of control. Previously the ADP Systems Security Officer.

information systems security
product

Item (chip, module, assembly, or equipment), technique, or service that performs or relates to information systems security. [G].

Information System Security

A catalogue issued quarterly by NSA that

Products and Services Catalogue	incorporates the EPL, the Degausser Products List (DPL), the Endorsed Tools List (ETL), the Endorsed Cryptographic Products List, the NSA Endorsed Data Encryption Standard (DES) Products List, the TEMPEST Preferred Products List (PPL), Off-line Systems, and other security product and service lists. [L].
Information Technology Security Evaluation Criteria (ITSEC)	A harmonized trusted product evaluation criteria developed by France, Germany, the Netherlands, and the United Kingdom. The first version of this document was released 2 May, 1990. [J].
Initial Product Assessment Report (IPAR)	The IPAR documents the results of the evaluation team's analysis of the security and design documentation of a vendor's product during the design analysis phase (DAP). Based on the team's findings, the product is assigned a candidate rating reflecting the highest class for which the product showed evidence of meeting all the TCSEC requirement. [J].
initialize	Setting the state of a cryptographic logic prior to key generation, encryption, or other operating mode. [G].
integration	The synthesis of a system's components to form either large components of the system or the system itself. [K].
integrity	(1) A subgoal of computer security which pertains to ensuring that data continues to be a proper representation of information, and that information processing resources continue to perform correct processing operations. (2) A subgoal of computer security which pertains to ensuring that information retains its original level of accuracy. <u>Data integrity</u> is that attribute of data relating to the preservation of (1) its meaning and completeness, (2) the consistency of its representation(s), and (3) its correspondence to what it represents. <u>System integrity</u> is that attribute of a system relating to the successful and correct operation of computing resources. [L].
integrity check value	Checksum that is capable of detecting malicious modification of an IS. [G].
integrity lock	A secure front end DBMS implementation method that adds mandatory security to a non-secure DBMS. The integrity of database records and their associated sensitivity labels are protected by message authentication codes. A mandatory access control policy is enforced for all database accesses by a front end filter. [J].

integrity policy	A security policy to prevent unauthorized users from modifying, viz., writing sensitive information. See also security policy. [J].
intelligence	Intelligence is the product resulting from the collection, evaluation, analysis, integration, and interpretation of all available information, which concerns one or more aspects of foreign nations or of areas of foreign operations, and which is immediately or potentially significant to military planning and operations. [J].
intelligence information	Information that is under the jurisdiction and control of the Director of Central Intelligence or a member of the Intelligence Community. [J].
interconnected accredited (A)IS	The interconnected accredited (A)IS view of a network is an operational perspective that recognizes that parts of network may be independently created, managed, and accredited. Each (A)IS is accredited to handle sensitive information at a single level or over a range between a minimum and a maximum level. [J].
interim approval	Temporary authorization granted by a designated approving authority for an IS to process classified information and information governed by 10 U.S.C. Section 2315 or 44 U.S.C. 3502(2) in its operational environment based on preliminary results of a security evaluation of the system. [G].
Interim Authority To Operate (IATO)	See interim approval.
internal security controls	Hardware, firmware, and software features within a system that restrict access to resources (hardware, software, and data) to only authorized subjects (persons, programs, or devices). [J].
internet 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. [G].
internet protocol	Standard protocol for transmission of data from source to destinations in packet-switched communications networks and interconnected systems of such networks. [G].

interpretation	Also, Interp. See criteria interpretation. [J].
intrusion	The act of violating the system security policy. [J].
Intrusion Countermeasure Equipment (ICE)	Automated audit analysis equipment that is used to detect and interrupt intrusions generally in real-time through comparison of current activity against profiles of expected activity and system policy. [J].
invariant	An assertion that is true in every reachable state. [J].
isolation	The containment of users and resources in a system in such a way that users and resources are separate from one another as well as from the protection controls of the operating system. [J].

K

kernel	See security kernel. [J].
key	Information (usually a sequence of random or pseudorandom binary digits) used initially to set up and periodically change the operations performed in crypto-equipment for the purpose of encrypting or decrypting electronic signals, for determining electronic counter-countermeasures patterns (e.g., frequency hopping or spread spectrum), or for producing other key. NOTE: "Key" has replaced the terms "variable," "key(ing) variable," and "cryptovvariable." [G].
key-auto-key	Cryptographic logic which uses previous key to produce key. [G].
key card	Paper card, containing a pattern of punched holes, which establishes the key for a specific cryptonet at a specific time. [G].
key encryption key	Key that encrypts or decrypts other key for transmission or storage. [G].
key list	Printed series of key settings for a specific cryptonet. NOTE: Key lists may be produced in list, pad, or printed tape format. [G].
key management	Process by which key is generated, stored, protected, transferred, loaded, used, and destroyed. [G].
key production key	Key that is used to initialize a keystream generator for the production of other electronically generated key. [G].
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. [G].
key tag	Identification information associated with certain types of electronic key. [G].

key tape	Punched or magnetic tape containing key. NOTE: Printed key in tape form is referred to as a key list. [G].
key updating	Irreversible cryptographic process for modifying key automatically or manually. [G].
keyboard attack	Extracting information from data storage media by executing software utilities, keystrokes, or other system resources executed from a keyboard. For example, disk and file recovery utilities and memory scavenging procedures can be used to carry out keyboard attacks. A countermeasure to keyboard attack is: to overwrite or remove data storage media, thereby making information unavailable to users employing normal capabilities. [I].
keying material	Key, code, or authentication information in physical or magnetic form. [G].

L

label	See sensitivity label. [J].
laboratory attack	Using sophisticated signal recovery equipment, in a laboratory environment, to recover stored information from data storage media. A countermeasure to laboratory attack is: to purge data storage media, rendering data unrecoverable by an effort commensurate with its sensitivity. [I].
lattice	A partially ordered set for which every pair of elements has a greatest lower bound and a least upper bound. [J].
least privilege	Principle that requires that each subject be granted the most restrictive set of privileges needed for the performance of authorized tasks. NOTE: Application of this principle limits the damage that can result from accident, error, or unauthorized use of an IS. [G].
least upper bound	In comparing two security levels S1 and S2, the unique security level that dominates S1 and S2 and is dominated by all other security levels that dominate both S1 and S2. See greatest lower bound. [J].
level	See security level. [J].
limited-access	Synonymous with access control. [G].
limited access authorization	Security access authorization to CONFIDENTIAL or SECRET information granted to non-U.S. citizens requiring such limited access in the course of their regular duties. [J].
limited dissemination	Restrictive controls for classified information established by an original classification authority to emphasize need-to-know protective measures available within the regular security system. [J].
limited maintenance	COMSEC maintenance restricted to fault isolation, removal, and replacement of plug-in assemblies. NOTE: Soldering or unsoldering usually is prohibited in limited maintenance. (See full maintenance.) [G].

line conduction	Unintentional signals or noise induced or conducted on a telecommunications or automated information system signal, power, control, indicator, or other external interface line. [G].
link encryption	Encryption of data in individual links of a telecommunications system. [G].
list-oriented	Computer protection in which each protected object has a list of all subjects authorized to access it. (See ticket-oriented.) [G].
local requirements	Those for which separate analysis of the individual TCB subsets suffice to determine compliance for the composite TCB. [J].
lock and key protection system	Protection system that involves matching a key or password with a specific access requirement. [G].
logic bomb	Resident computer program that triggers an unauthorized act when particular states of an IS are realized. [G].
logical completeness	Means for assessing the effectiveness measure and degree to which a set of security and access control mechanisms meets the requirements of security specifications. [G].
long title	Descriptive title of a COMSEC item. [G].
loophole	An error of omission or oversight in software or hardware that permits circumventing the system security policy. [J].
low probability of detection	Result of measures used to hide or disguise intentional electromagnetic transmissions. [G].
low probability of intercept	Result of measures to prevent the intercept of intentional electromagnetic transmissions. [G].
low-water mark	Of two or more security levels, the least of the hierarchical classifications, and the set intersection of the non-hierarchical categories. See high-water mark. [J].

M

machine cryptosystem	Cryptosystem in which cryptographic processes are performed by crypto- equipment. [G].
magnetic remanence	<p>Magnetic representation of residual information that remains on a magnetic medium after the medium has been erased or overwritten.</p> <p>NOTE: Magnetic remanence refers to data remaining on magnetic storage media after removal of the power or after degaussing. [G].</p>
maintenance hook	<p>Special instructions in software to allow easy maintenance and additional feature development.</p> <p>NOTE: Maintenance hooks are not clearly defined during access for design specification. Since maintenance hooks frequently allow entry into the code at unusual points or without the usual checks, they are a serious security risk if they are not removed prior to live implementation. Maintenance hooks are special types of trap doors. [G].</p>
maintenance key	Key intended only for off-the-air in-shop use. [G].
malicious logic	<p>Hardware, software, or firmware that is intentionally included in an IS for an unauthorized purpose.</p> <p>NOTE: Trojan horse is a form of malicious logic. [G].</p>
Mandatory Access Control (MAC)	Means of restricting access to objects based on the sensitivity (as represented by a label) of the information contained in the objects and the formal authorization (i.e., clearance) of subjects to access information of such sensitivity. (See discretionary access control.) [G].
mandatory modification	<p>Change to a COMSEC end item that the -National Security Agency requires to be completed and reported by a specified date.</p> <p>NOTE: This type of modification should not be confused with modifications that are optional to the National Security Agency, but have been adjudged mandatory by a given department or agency. The latter modification may</p>

have an installation deadline established and controlled solely by the user's headquarters. [G].

mandatory security policy

A policy that is based on constraints imposed by a recognized authority for the protection of sensitive information and applied uniformly to all users of a computing system. [J].

manipulative communications deception

Alteration or simulation of friendly telecommunications for the purpose of deception.

NOTE: Manipulative communications deception may involve establishment of bogus communications structures, transmission of deception messages, and expansion or creation of communications schedules on existing structures to display an artificial volume of messages. (See communications deception and imitative communications deception.) [G].

manual cryptosystem

Cryptosystem in which the cryptographic processes are performed manually without the use of crypto-equipment or automanual devices. [G].

manual remote rekeying

Procedure by which a distant crypto -equipment is rekeyed electrically, with specific actions required by the receiving terminal operator. [G].

marking

The indication of the security classification of a document. [J].

masquerading

Synonymous with spoofing. [G].

master crypto-ignition key

Crypto-ignition key that is able to initialize crypto-ignition key, when interacting with its associated crypto--equipment. [G].

material symbol

Communications circuit identifier used for key card resupply purposes. [G].

memory bounds

Limits in the range of storage addresses for a protected region in the memory of an IS. [G].

memory scavenging

Searching through data storage to collect residue thereby acquiring data. Data storage may be records, blocks, pages, segments, files, directories, words, bytes, fields, or peripheral devices such as printers or video displays or others. [I].

message authentication code	Data element associated with an authenticated message which allows a receiver to verify the integrity of the message. [G].
message externals	Non-textual (outside the message text) characteristics of transmitted messages. [G].
message indicator	Sequence of bits transmitted over a telecommunications system for the purpose of crypto-equipment synchronization. NOTE: Some off-line cryptosystems, such as the KL-51 and one-time pad systems, employ message indicators to establish decryption starting points. [G].
metadata	(1) Data referring to other data; data (such as data structures, indices, and pointer) that are used to instantiate an abstraction (such as "process," "task," "segment," "file," or "pipe"). (2) A special database, also referred to as a data dictionary, containing descriptions of the elements (e.g., relations, domains, entities, or relationships) of a database. [J].
mimicking	Synonymous with spoofing. [G].
mission	A specific task with which a person, or group of individuals, or organization is entrusted to perform. [K].
mission criticality	The property that data, resources, and processes may have, which denotes that the importance of that item to the accomplishment of the mission is sufficient to be considered an enabling/disabling factor. [K].
mobile COMSEC facility	COMSEC facility that can be readily moved from one location to another. [G].
mode of operation	Description of the conditions under which an IS operates, based on the sensitivity of data processed and the clearance levels and authorizations of the users. NOTE: Five modes of operation are authorized for an IS processing information and for networks transmitting information. (See compartmented mode, dedicated mode, multilevel mode, partitioned security mode, and system - high mode.) [G].

model	An abstraction or simplification of reality, the purpose of which is to capture key aspects of the behavior of the reality. [J].
monolithic TCB	A TCB that consist of a single TCB subset. [J].
multi-level device	Device that is trusted to properly maintain and separate data of different security levels. [G].
multi-level mode	<p>IS security 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:</p> <ol style="list-style-type: none">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.c. All users have a valid need-to-know only for information to which they have access. [G].
Multilevel Secure (MLS)	A class of system containing information with different sensitivities that simultaneously permits access by users with different security clearances and need-to-know, but prevents users from obtaining access to information for which they lack authorization. [J].
multi-level security (mode)	<ol style="list-style-type: none">1. Concept of processing information with different classifications and categories that simultaneously permits access by users with different security clearances, but prevents users from obtaining access to information for which they lack authorization. [G].2. Data on your information system is at two or more classification levels and not all users have the clearance for the highest classification of data.3. An IS is operating in the multilevel mode when one or more of its users do not possess the proper security clearance for accessing the most sensitive classified data processed and stored by the IS. Data classification labels maintained by the system can be trusted. [H].

mutual suspicion

Condition in which two entities need to rely upon each other to perform a service, yet neither entity trusts the other to properly protect shared data. [G].

mutually suspicious

The state that exist between interacting processes (subsystems or programs) in which neither process can expect the other process to function securely with respect to some property. [J].

N

named object	An object which is directly manipulatable at the TCB interface. The object must have meaning to more than one process. [J].
National Computer Security Center (NCSC)	Originally named the DoD Computer Security Center, the NCSC is responsible for encouraging the widespread availability of trusted computer systems throughout the Federal Government. To this end, the NCSC has published the TCSEC and a series of guidelines on trusted systems technology. The NCSC is a part of NSA. [J].
National Institute of Standards and Technology (NIST)	The U.S. Government agency responsible for standards and technology. Their National Computer Systems Laboratory conducts research and provides scientific and technical services to aid Federal agencies in the selection, acquisition, application, and use of computer technology. [J].
National Security Agency (NSA)	The parent organization of the NCSC. The NSA's main charter is signals intelligence (SIGINT) and information security (INFOSEC) for the U.S. Government, which includes COMSEC and COMPUSEC. The NSA sponsors the Commercial COMSEC Endorsement Program (CCEP). [J].
National Security Directive 42 (NSD 42)	Signed by President Bush on 5 July 1990, this directive is entitled "National Policy for the Security of National Security Telecommunications and Information systems." It provides initial objectives, policies, and an organizational structure to guide the conduct of activities to secure national security systems from exploitation; establishes a mechanism for policy development and dissemination; and assigns responsibilities for implementation. [A].
national security information	Information that has been determined, pursuant to Executive Order 12356 or any predecessor order, to require protection against unauthorized disclosure, and that is so designated. [G].
national security systems	Telecommunications and automated information systems operated by the U.S. Government, its contractors, or its agents, that contain classified information or, as set forth

in 10 U.S.C. Section 2315, that involves intelligence activities, involves cryptologic activities related to national security, involves command and control of military forces, involves equipment that is an integral part of a weapon or weapon system, or involves equipment that is critical to the direct fulfillment of military or intelligence missions. [G].

NATO information

Information bearing NATO marking, indicating the information is the property of NATO, access to which is limited to representatives of NATO and its member nations unless proper NATO authority has been obtained to release outside of NATO. [J].

need-to-know

Access to, or knowledge or possession of, specific information required to carry out official duties. [G].

net control station

Terminal in a secure telecommunications net responsible for distributing key in electronic form to the members of the net. [G].

network

A communications medium and all components attached to that medium whose responsibility is the transference of information. Such components may include AISs, packet switches, telecommunications controllers, key distribution centers, and technical control devices. [J].

network architecture

The set of layers and protocols (including formats and standards that different hardware/software must comply with to achieve stated objectives) which define a Network. [J].

network component

A network subsystem which is evaluable for compliance with the trusted network interpretations, relative to that policy induced on the component by the overall network policy. Network components can be developed and evaluated to enforce combinations of MAC, DAC, I&A, and Audit policies. [J].

network connection

A network connection is any logical or physical path from one host to another that makes possible the transmission of information from one host to the other. An example is a TCP connection. [J].

network front-end

Device that implements the needed security-related protocols to allow a computer system to be attached to a network. [G].

network reference monitor	Access control concept that refers to an abstract machine that mediates all access to objects within a network by subjects within the network. (See reference monitor.) [G].
network security	Protection of networks and their services from unauthorized modification, destruction, or disclosure, and provision of assurance that the network performs its critical functions correctly and there are no harmful side-effects. NOTE: Network security includes providing for data integrity. [G].
network security architecture	A subset of network architecture specifically addressing security-relevant issues. [J].
Network Security Officer (NSO)	Individual formally appointed by a designated approving authority to ensure that the provisions of all applicable, directives are implemented throughout the life cycle of an automated information system network. (See information system security officer.) [G].
network security services	Security features provided by a network including those typically assumed by a stand-alone secure system (e.g., Communications Field Integrity, Non-repudiation, Selective Routing). [J].
network sponsor	The individual or organization that is responsible for stating the security policy enforced by the network, for designing the network security architecture to properly enforce that policy, and for ensuring that the network is implemented in such a way that the policy is enforced. For commercial, off-the-shelf systems, the network sponsor will normally be the vendor. For a fielded network system, the sponsor will normally be the project manager or system administrator. [J].
network system	System that is implemented with a collection of interconnected network components. NOTE: A network system is based on a coherent security architecture and design. [G].
network trusted computing base	Totality of protection mechanisms within a network system, including hardware, firmware, and software, the

combination of which is responsible for enforcing a security policy. (See trusted computing base.) [G].

no-lone zone	Area, room, or space which, when manned, must be occupied by two or more appropriately cleared individuals who remain within sight of each other. (See two person integrity.) [G].
non-cooperative remote rekeying	Synonymous with automatic remote rekeying. [G].
non-hierarchical category	In Mandatory Access Control non-hierarchical refers to categories of special access requirements imposing 'need-to-know' or access controls beyond those normally provided for access to sensitive or classified information. These categories are non-hierarchical in the sense that access to one category does not automatically imply access to another. Compare Hierarchical-level. [J].
non-repudiation	Method by which the sender of data is provided with proof of delivery and the recipient is assured of the sender's identity so that neither can later deny having processed the data. [G].
non-secret encryption	Synonymous with public key cryptography. [G].
NTCB partition	The 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. [J].
null	Dummy letter, letter symbol, or code group inserted in an encrypted message to delay or prevent its decryption or to complete encrypted groups for transmission or transmission security purposes. [G].

O

object	<p>1. Passive entity that contains or receives information.</p> <p>NOTE: Access to an object implies access to the information it contains. Examples of objects are: records, blocks, pages, segments, files, directories, directory trees and programs, as well as bits, bytes, words, fields, processors, video displays, keyboards, clocks, printers, and network nodes. [G].</p> <p>2. Any passive entity that contains or receives information (e.g., files, directories, records, locks, pages, segments, programs, video displays, printers). Access to an object implies access to the information it contains. [H].</p>
object reuse	<p>Reassignment of a storage medium (e.g., page frame, disk sector, magnetic tape) that contained one or more objects, after ensuring that no residual data remained on the storage medium. [G].</p>
off-line cryptosystem	<p>Cryptosystem in which encryption and decryption are performed independently of the transmission and reception functions. [G].</p>
off-line systems	<p>A variety of off-line capabilities that NSA can provide to meet customer requirements. Off-line refers to those cryptosystems where encryption and decryption are performed separately from the transmitting and receiving functions. [L].</p>
one-part code	<p>Code in which plain text elements and their accompanying code groups are arranged in alphabetical, numerical, or other systematic order, so that one listing serves for both encoding and decoding.</p> <p>NOTE: One-part codes are normally small codes that are used to pass small volumes of low-sensitivity information. [G].</p>
one-time cryptosystem	<p>Cryptosystem employing key which is used only once. [G].</p>
one-time pad	<p>Manual one-time cryptosystem produced in pad form. [G].</p>

one-time password	A password scheme in which information and/or a mathematical function available to the user and the system is used to generate a new password for each log-in. See Challenge/Response. [J].
one-time tape	Punched paper tape used to provide key streams on a one-time basis in certain machine cryptosystems. [G].
on-line cryptosystem	Cryptosystem in which encryption and decryption are performed in association with the transmitting and receiving functions. [G].
open security environment	Environment that does not provide sufficient assurance that applications and equipment are protected against the introduction of malicious logic prior to or during the operation of a system. [G].
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. [G].
operating condition	Refers to whether equipment is in working order. [I].
operating environment	The combination of hardware, firmware, operating system software, and application software being evaluated for certification. Once certified, the operating environment will become a Trusted Computing Base (TCB). [M].
operational data security	Protection of data from either accidental or unauthorized intentional modification, destruction, or disclosure during input, processing, or output operations. [G].
operational key	Key intended for use on-the-air for protection of operational information or for the production or secure electrical transmission of key streams. [G].
operational waiver	Authority for continued use of unmodified COMSEC end-items, pending the completion of a mandatory modification. [G].
operations code	Code composed largely of words and phrases which are suitable for general communications use. [G].
operations security	Process denying to potential adversaries information about capabilities and/or intentions by identifying, controlling and protecting generally unclassified evidence of the planning and execution of sensitive activities. [G].

optional modification	National Security Agency approved modification that is not required for universal implementation by all holders of a COMSEC end-item. NOTE: 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. [G].
Orange Book	Synonymous with DoD Trusted Computer System Evaluation Criteria. DOD 5200.28-STD, dtd Dec 85. [G].
organizational maintenance	Limited maintenance performed by a user organization. [G].
organizational security policy	Set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information. [J].
overt channel	Communications path within a computer system or network that is designed for the authorized transfer of data. (See covert channel.) [G].
over-the-air key distribution	Providing electronic key via over-the-air rekeying, over-the-air key transfer, or cooperative key generation. [G].
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. [G].
over-the-air rekeying	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. [G].
overwrite procedure	Process which removes or destroys data recorded on an IS storage medium by writing patterns of data over, or on top of, the data stored on the medium. [G].
overwriting	Writing data in the same storage location currently occupied by other data.
owner	User granted privileges with respect to security attributes and privileges affecting specific subjects and objects. [J].

P

parity	Set of bits used to determine whether a block of data (key or data stored in computers) has been intentionally or unintentionally altered. [G].
partially ordered	<p>A dominance relation on a set S (e.g., the usual dominance relationship on security labels) is called a partial ordering if it satisfies the following properties:</p> <p>Reflexive: For all A in S: A dominates A</p> <p>Antisymmetric: For all A, B in S: if A dominates B and B dominates A then $A = B$</p> <p>Transitive: For all A, B, C in S: if A dominates B and B dominates C then A dominates C</p> <p>If it is also true that all A, B in S either A dominates B or B dominates A, then the relation is a total ordering. The usual ordering of hierarchical security levels forms a total ordering. However, security levels with categories, while still partially ordered, are not totally ordered because if categories A and B are distinct neither dominates the other. See Hierarchical Level, Non-hierarchical Category. [J].</p>
partitioned security mode	<p>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.</p> <p>NOTE: This security mode encompasses the compartmented mode and applies to non-intelligence DoD organizations and DoD contractors. [G].</p>
passive	(1) A property of an object or network object that it lacks logical or computational capability and is unable to change the information it contains. (2) Those threats to the confidentiality of data which, if realized, would not result in any unauthorized change in the state of the intercommunicating systems (e.g., monitoring and/or recording of data). [J].
passphrase	Sequence of characters, longer than the acceptable length of a password, that is transformed by a password system into a virtual password of acceptable length. [G].

password	Protected/private character string used to authenticate an identity or to authorize access to data. [G].
password aging	The automated process ensuring that password lifetimes are acceptably short. Users are forced by the Identification & Authentication mechanism to change or accept new passwords on a periodic basis. [J].
penetration	Unauthorized act of bypassing the security mechanisms of a cryptographic system or IS. [G].
penetration signature	The characteristics or identifying marks that may be produced by a penetration. [J].
penetration study	A study to determine the feasibility and methods for defeating [the security] controls of a system. [J].
penetration testing	Security testing in which evaluators attempt to circumvent the security features of an IS based on their understanding of the system design and implementation. [G].
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.) [G].
periods processing	Processing of various levels of classified and unclassified information at distinctly different times. NOTE: Under periods processing, the system must be purged of all information from one processing period before transitioning to the next when there are different users with differing authorizations. [G].
permissions	A description of the type of authorized interaction a subject can have with an object. Permissions include: read, write, execute, add, modify, delete.[J].
permuter	Device used in a crypto-equipment to change the order in which the contents of a shift register are used in various nonlinear combining circuits. [G].
Personal Identification Number (PIN)	A personal number used to authenticate a user in certain security. Procedures for screening all individuals background checks, etc., to ensure that they can be given a level of trust commensurate with their duties. [J].

philosophy of protection	An informal description of the overall design of a system that delineates each of the protection mechanisms employed. A combination (appropriate to the evaluation class) of formal and informal techniques is used to show that the mechanisms are adequate to enforce the security policy. [J].
physical security	Action taken to protect installations, personnel, equipment, computer media, documents, etc. from damage, loss, theft, and/or unauthorized access. [H].
piggyback	Unauthorized access that is gained to an ADP system through another user's legitimate connection. [J].
plain text	Unencrypted information. [G].
playback	An attack in which a valid, possibly encrypted, message is saved and replayed to duplicate the original effect. Time stamping can be used to limit this threat. [J].
polyinstantiate	In databases, to create multiple instances of data records with the same primary key at different security levels. [J].
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. [G].
Preferred Products List (PPL)	A list of commercially produced equipment that meets TEMPEST and other requirements prescribed by NSA. This list is included in the Information Systems Security Products and Service Catalogue Supplement; Oct. 93. [J].
Preliminary Technical Review (PTR)	The PTR occurs during the proposal review phase of the NSA evaluation process. In this phase the NSA determines whether it will actually evaluate a product. During the PTR the vendor and NSA discuss the technical aspects of the product with respect to its potential evaluation. [J].
preproduction model	Version of a crypto-equipment that employs standard parts and is in final mechanical and electrical form suitable for complete evaluation of form, design, and performance. NOTE: Preproduction models are often referred to as E-model equipment. [G].

primitive	An ordering relation between TCB subsets based on dependency (see "depends" above). A TCB subset B is more primitive than a second TCB subset A (and A is less primitive than B) if (a) A directly depends on B or (b) a chain of TCB subsets from A to B exists such that each element of the chain directly depends on its successor in the chain. [J].
print suppression	Eliminating the display of characters in order to preserve their secrecy. NOTE: An example of print suppression is not displaying the characters of a password as it is keyed at the input terminal. [G].
privacy	(1) The ability of an individual or organization to control the collection, storage, sharing, and dissemination of personal and organizational information. (2) The right to insist on adequate security of, and to define authorized users of information or systems. [J].
privacy system	Commercial encryption system that affords telecommunications limited protection to deter a casual listener, but cannot withstand a technically competent cryptanalytic attack. [G].
privilege	The ability to perform some operation that is not available without the appropriate privilege. [J].
privileged instructions	A set of instructions (e.g., interrupt handling or special computer instructions to control features such as storage protection features) generally executable only when the automated system is operating in the executive state. [J].
procedural security	Synonymous with administrative security. [J].
process	A program in execution on a processor which represents a scheduling and accounting (and sometimes a concurrency and recovery) entity in a computer system. [J].
product	A product is a developed system component that may be used in a variety of operational environments. [L].
production model	Crypto-equipment in its final mechanical and electrical form of production design made by use of production tools, jigs, fixtures, and methods using standard parts. [G].

profile	<ol style="list-style-type: none">1. Detailed security description of the physical structure, equipment component, location, relationships, and general operating environment of an IS. [G].2. Associates each user with a list of protected objects that the user may access.
profile assurance	Measure of confidence in the technical soundness of a protection profile. [J].
propagation of access rights	In the Discretionary Access Control , this refers to the transfer of access rights to an object from one individual to another. [J].
proposal review phase	The first phase of the NSA evaluation process where the NSA determines weather it will actually evaluate a product that has been submitted for evaluation. It is during this phase that the vendor and the NSA introduce themselves to each other and the vendor submits a proposal package regarding the product they wish to have evaluated. Based on the analysis of the proposal package and a Preliminary Technical Review (PTR) the NSA determines weather it will evaluate the product. [J].
proprietary information	<p>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 have been clearly identified and properly marked as proprietary information, trade secrets or company confidential information.</p> <p>NOTE: Trade secrets constitute the whole or any portion or phase of any technical information, design process, procedure, formula or improvement that is not generally available to the public, that a company considers company confidential and that could give or gives an advantage over competitors who do not know or use the trade secret. [G].</p>
protected communications	Telecommunications deriving their protection through use of type 2 products or data encryption standard equipment. (See secure communications.) [G].

protected distribution system	Wireline or fiber-optic telecommunications system that includes terminals and adequate acoustic, electrical, electromagnetic, and physical safeguards to permit its use for the unencrypted transmission of classified information. [G].
protection bits	A bit vector, where each bit represents a type of access. The most common example is the UNIX nine-bit vector reflecting read, write, and execute access to be granted to the object's owner, a group, and everyone else. [H].
protection critical portions of the TCB	These portions of the TCB whose normal function is to deal with the control of access between subjects. Their correct operation is essential to the protection of the data on the system. [J].
protection equipment	Type 2 product or data encryption standard equipment that the National Security Agency has endorsed to meet applicable standards for the protection of telecommunications or automated information systems containing national security information. [G].
protection philosophy	Informal description of the overall design of an IS that delineates each of the protection mechanisms employed. NOTE: Combination, appropriate to the evaluation class, of formal and informal techniques used to show the mechanisms are adequate to enforce the security policy. [G].
protection profile	Statement of security criteria; shared by IT product producers, consumers, and evaluators; built from functional, development assurance, and evaluation assurance requirements; to meet identified security needs through the development of conforming IT products. [J].
protection profile family	Two or more protection profiles with similar functional requirements and rational sections but with different assurance requirements. [J].
protection ring	One of a hierarchy of privileged modes of an IS that gives certain access rights to user programs and processes authorized to operate in a given mode. [G].
protective packaging	Packaging techniques for COMSEC material which discourage penetration, reveal that a penetration has occurred or was attempted, or inhibit viewing or copying

	of keying material prior to the time it is exposed for use. [G].
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. [G].
protective technology/package incident	Any penetration of information system security protective technology or packaging, such as a crack, cut, or tear. [G].
protocol	Set of rules and formats, semantic and syntactic, that permits entities to exchange information. [G].
prove a correspondence	Provide a formal correspondence, using a formal reasoning system (e.g., typed lambda calculus) between the levels of abstraction. Note: This involves proving that required properties continue to hold under the interpretation given in the formal correspondence. [J].
public cryptography	Body of cryptographic and related knowledge, study, techniques, and applications that is, or intended to be, in the public domain. [G].
public key cryptography	Type of cryptography in which the encryption process is publicly available and unprotected, but in which a part of the decryption key is protected so that only a party with knowledge of both parts of the decryption process can decrypt the cipher text. NOTE: Commonly called non-secret encryption in professional cryptologic circles. FIREFLY is an application of public key cryptography. [G].
public object	An object for which the ADP system implementation permits all untrusted subjects to perform non-modify operations (e.g., read, execute) on the object's contents and attributes, but permits only trusted subjects to modify the object's contents or attributes, and permits only trusted subjects to create or destroy such objects. [J].
purge	Removal of data from an IS, its storage devices, or other peripheral devices with storage capacity in such a way that the data may not be reconstructed.'

NAVSO P-5239-02
JUNE 1995

NOTE: An IS must be disconnected from any external network before a purge. (See clearing.) [G].

purging

Rendering stored information unrecoverable by laboratory attack. [I].

purging magnetic media

A procedure used to totally and unequivocally erase or overwrite all information stored on magnetic media. Purging is one prerequisite to declassification of magnetic media. [J].

Q

QUADRANT

Short name referring to technology which provides
tamper-resistant protection to crypto-equipment. [G].

R

rainbow series	The series of standards and guidelines published by the NCSC. Each document is published with a different color, thus the term "rainbow" series. [J].
RAMP Audit	A review of the RAMP Evidence to ascertain, based on a suitable representative sample, that only approved changes are implemented, that all Configuration Items are updated consistently, and that Security Analysis is performed satisfactorily. in addition to the required RAMP Audits performed by the VSAs, aperiodic RAMP Audits may be performed by the TPOCs. [J].
RAMP Cycle	The period of time between the dates of two consecutive EPL entries. [J].
RAMP Evidence	The record of Security Analysis. It serves to establish accountability for each change and to provide justification for the inclusion of each of those changes. For each change, RAMP Evidence consists of the issues and conclusions of the Security Analysis and all the information maintained by the vendor's configuration management system (e.g., a description of the change; what Configuration Items were affected; the status of the changes to the Configuration Items, and accountability for the change). [J].
RAMP Product	The complete set of Configuration Items constituting the current RAMP action. The original evaluated product is the starting point for the first RAMP Product. [J].
randomizer	Analog or digital source of unpredictable, unbiased, and usually independent bits. NOTE: Randomizers can be used for several different functions, including key generation or to provide a starting state for a key generator. [G].
rating	The evaluation class that can be assigned to a trusted product. There are seven TCSEC ratings: D, C1, C2, B1, B2, B3, and A1 ordered hierarchically with A1 providing the most comprehensive security. There are four subsystem ratings, D, D1, D2, D3 ordered hierarchically. Network components are given one or more of the following rating based on the functionality they provide:

M (Mandatory Access Control), A (Audit), I (Identification and Authentication), and D (Discretionary Access Control). [J].

Rating Maintenance Phase (RAMP)	The phase of the Trusted Product Evaluation Program that follows the Formal Evaluation Phase. RAMP consist of a series of rating-maintenance actions (RAMP Cycles) that assess the compliance with TCSEC requirements of updated versions of the product and allow those versions to be listed on the EPL. During RAMP, the vendor performs the majority of the work to determine that changes to the product maintain the previously attained rating. [J].
Rating Maintenance Plan (RM PLAN)	The vendor document that describes the mechanisms, procedures, and tools used to meet the RAMP requirements. The RM-Plan is approved by the NSA. The first RM-Plan must be approved before the Formal Evaluation Phase begins. The procedures outlined in the approved RM-Plan shall be in place prior to the testing TRB of the original evaluation. [J].
Rating Maintenance Report (RMR)	A summary of RAMP Evidence that is submitted to the TRB. [J].
reaccreditation	<p>The official management decision to continue operating a previously accredited system.</p> <p>Note: Reaccreditation occurs (1) periodically, regardless of system change (based on policy (e.g., DoD 5200.28 requires a 3 year reaccreditation cycle)) or (2) if major changes have been made to some aspect of the system that impact security. [K].</p>
read	Fundamental operation in an IS that results only in the flow of information from an object to a subject. (See access type.) [G].
read access	Permission to read information in an IS. [G].
real-time reaction	Immediate response to a penetration attempt that is detected and diagnosed in time to prevent access. [G].
recertification	A reassessment of the technical and nontechnical security features and other safeguards of a system made in support of the reaccreditation process.

Note: The level of effort for recertification will depend on the nature of changes (if any) made to the system and any potential changes in the risk of operating the system (e.g., changes in the threat environment may affect the residual risk). [K].

recovery procedures	Actions necessary to restore data files of an IS and computational capability after a system failure. [G].
RED	Designation applied to telecommunications and automated information systems, plus associated areas, circuits, components, and equipment which, when classified plain text signals are being processed therein, require protection during electrical transmission. [G].
RED book	Alternate name for Trusted Network Interpretation (TNI) of the TCSEC originating from its red cover. [J].
RED/BLACK concept	Separation of electrical and electronic circuits, components, equipment, and systems that handle classified plain text (RED) information, in electrical signal form, from those which handle unclassified (BLACK) information in the same form. [G].
RED key	Unencrypted key. (See BLACK key.) [G].
RED signal	Telecommunications or automated information systems signal that would divulge classified information if recovered and analyzed. NOTE: RED signals may be plain text, key, subkey, initial fill, control, or traffic flow related information. [G].
reference monitor	Access control concept that refers to an abstract machine that mediates all accesses to objects by subjects. [G].
reference validation mechanism	Portion of a trusted computing base, the normal function of which is to control access between subjects and objects, and the correct operation of which is essential to the protection of data in the system. NOTE: This is the implementation of reference monitor. [G].
regrade	This is to assign a higher or lower security classification to an item of classified material. An "upgrade" results in a higher classification; a "downgrade" results in a lower classification. [J].

release marking	Authorized marking placed on a document by its originator for the purpose of imposing restrictions on dissemination of the document and the information it contains. [J].
release prefix	Prefix expended to the short title of United States produced keying material to indicate its foreign releasability. NOTE: "A" designates material that is releasable to specific allied nations and "US" designates material intended exclusively for United States use. [G].
reliability	The extent to which a system can be expected to perform its intended function with required precision. [J].
remanence	Residual information that remains on storage media after erasure, [G] or after use of insufficient purging procedures. (See magnetic remanence.).
remote rekeying	Procedure by which a distant crypto- equipment is rekeyed electrically. (See automatic remote rekeying and manual remote rekeying.) [G].
removal of external marking	The removal of external markings is a physical and administrative process applied to computer data storage media after classified, and/or sensitive but unclassified, information has been purged or declassified. [I].
repair action	National Security Agency 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. NOTE: 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. [G].
repudiation	The denial of either the origin (sending) or receipt of a message. An example of the former is denying a purchase order was issued; an example of the latter is denying payment was received. [J].

reserve keying material	Key held to satisfy unplanned needs. (See contingency key.) [G].
residual risk	Portion of risk that remains after security measures have been applied. [G].
residue	Data left in storage after automated information processing operations are complete, but before degaussing or overwriting has taken place. [G].
resource	Anything used or consumed while performing a function. The categories of resources are: time, information, objects (information containers), or processors (the ability to use information). Specific examples are: CPU time; terminal connect time; amount of directly-addressable memory; disk space; number of I/O requests per minute, etc. [J].
resource encapsulation	Method by which the reference monitor mediates accesses to an IS resource. NOTE: Resource is protected and not directly accessible by a subject. Satisfies requirement for accurate auditing of resource usage. [G].
Responsible Corporate Officer (RCO)	A person empowered financially and legally to commit resources in support of RAMP and support the technical role of the VSAs, including denial of TCB changes. [J].
restricted area	Any area to which access is subject to special restrictions or controls for reasons of security or safeguarding of property or material. [J].
restricted data	All data or information concerning: (i) design, manufacture, or utilization of atomic weapons; (ii) the product of special nuclear material; or (iii) the use of special nuclear material in the material production of energy, but not to include data declassified or removed from the RESTRICTED DATA category pursuant to Section 142 of the Atomic Energy Act (see FORMALLY RESTRICTED DATA). [J].
risk	The probability that a particular threat will exploit a particular vulnerability of the system. [J].
risk analysis	Synonymous with risk assessment. [G].
risk assessment	Process of analyzing threats to and vulnerabilities of an information system, and the potential impact that the loss

of information or capabilities of a system would have on national security and using the analysis as a basis for identifying appropriate and cost-effective measures. [G]. Risk analysis is part of risk management, which is used to minimize risk by specifying security measures commensurate with the relative value of the resources to be protected, the vulnerabilities of those resources, and the identified threats against them.

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. [G].
risk management	Process concerned with the identification, measurement, control, and minimization of security risks in information systems. [G]. It includes risk analysis, cost benefit analysis, countermeasure selection, security test and evaluation, countermeasure implementation, and system review.
role	Specific job function explicitly supported by an (A)IS. Examples are: normal user, operator, system administrator, security officer, database administrator, network manager, etc. Each of these role is assigned an explicit set of privileges allowing the user performing the role to accomplish their intended tasks. [J].
rules of operation	Descriptions of key ideas associated with the design of the security-enforcement mechanisms in a trusted computing system. Rules of operation typically describe basic state transformations that accomplish necessary access control checks. [J].

S

safeguard	See Security Safeguards. [J].
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 person. [G].
sample key	Key intended for off-the-air demonstration use only. [G].
sanitize	To remove or edit classified or sensitive data so that what remains is of a lower classification or sensitivity than the original data. [G].
scavenging	Searching through object residue to acquire data. [G].
scratch pad store	Momentary key storage in crypto- equipment. [G].
secrecy	Synonymous with confidentiality. [J].
SECRET (S)	The designation that shall be applied only to information or material the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security. Examples of "serious damage" include disruption of foreign relations significantly affecting the national security, significant impairment of a program or policy directly related to the national security, revelation of significant military plans or intelligence operations, and compromise of significant scientific or technological developments relating to national security. [J].
secure attention key	A key to generate an attention character. (Also Hot Key) See Attention Character. [J].
secure communications	Telecommunications deriving security through use of type I products and/or protected distribution systems. [G].
Secure Concept of Operations (SCOPS)	A description of how an organization will conduct its business (or perform its mission) from a security perspective. It describes how security will be implemented in an organization's operational environment including all the mechanisms, both technical and non-

	technical, used to enforce the organizational security policies and procedures. [J].
secure configuration management	The set of procedures appropriate for controlling changes to a system's hardware and software structure for the purpose of ensuring that changes will not lead to violations of the system's security policy. [J].
secure operating system	Resident software that controls hardware and other software functions in an IS to provide a level of protection or security appropriate to the classification, sensitivity, and/or criticality of the data and resources it manages. [G].
secure state	Condition in which no subject can access any object in an unauthorized manner. [G].
secure subsystem	Subsystem that contains its own implementation of the reference monitor concept for those resources it controls. NOTE: Secure subsystem must depend on other controls and the base operating system for the control of subjects and the more primitive system objects. [G].
secure system	An (A)IS that satisfies an associated system security policy. [J].
security	Establishment and maintenance of protective measures intended to ensure a state of inviolability from hostile acts and influences, design deficiencies, system/component failure/malfunction, or unintentional misuse. [K].
security analysis team	The individual or individuals (e.g., VSAs, TPOCs, additional evaluators) responsible for performing the Security Analysis and presentation and defense of the RAMP Evidence before the TRB. [J].
security architecture	A detailed description of all aspects of the system that relate to security, along with a set of principles to guide the design. A security architecture describes how the system is put together to satisfy the security requirements. Note: A security architecture is basically an architectural overlay that addresses security. It is increasingly important in distributed systems, since there are many ways in which security functions can be distributed and care is needed to ensure that they work together. [K].

security attribute	Any piece of information that may be associated with a controlled entity or user for the purpose of implementing a security policy. [J].
security audit	An examination of data security procedures and measures for the purpose of evaluating their adequacy and compliance with established policy. [J].
security classification	The sensitivity of the information. See Security Level. [J].
security clearance	A security level associated with an individual having a recognized requirement to access classified information at that level or below. The security level assigned is based on the results of interviews and background investigations conducted by investigative organizations. [J].
security CONOPS	A high-level description of how the system operates and a general description of the security characteristics of the system, such as user clearances, data sensitivity, and data flows. [K].
security critical mechanisms	Those security mechanisms whose correct operation is necessary to ensure that the security policy is enforced. [J].
security evaluation	An evaluation done to assess the degree of trust that can be placed in systems for the secure handling of sensitive information. One type, a product evaluation, is an evaluation performed on the hardware and software features and assurance of a computer product from a perspective that excludes the application environment. The other type, a system evaluation, is done for the purpose of assessing a system's security safeguards with respect to a specific operational mission and is a major step in the certification and accreditation process. [J].
security fault analysis	Assessment, usually performed on information system hardware, to determine the security properties of a device when hardware fault is encountered. [G].
security features	The security-relevant functions, mechanisms, and characteristics of (A)IS hardware and software. Security features are a subset of (A)IS security safeguards. [J].

Security Features Users Guide (SFUG)	A document necessary to satisfy the requirements of any TCSEC class. The SFUG is directed towards the general users of the system. It describes the protection mechanisms provided by the TCB, contains the guidance on their use, and describes how they interact with one another. [J].
security filter	IS trusted subsystem that enforces security policy on the data that passes through it. [G].
security flaw	Error of commission or omission in an IS that may allow protection mechanisms to be bypassed. [G].
security flow analysis	A security analysis performed on a formal system specification that locates potential flows of information within the system which are not permitted by the system security policy. [J].
security inspection	Examination of an IS to determine compliance with security policy, procedures, and practices. [G].
security kernel	Hardware, firmware, and software elements of a trusted computing base that implement the reference monitor concept. NOTE: Security kernel must mediate all accesses, be protected from modification, and be verifiable as correct. [G].
security label	Piece of information that represents the sensitivity of a subject or object, such as its hierarchical classification (CONFIDENTIAL, SECRET, TOP SECRET) together with any applicable non-hierarchical security categories (e.g., sensitive compartmented information, critical nuclear weapon design information). (See information label and sensitivity label.) [G].
security level	The combination of a hierarchical classification and a set of nonhierarchical categories that represents the sensitivity of information. [J].
security measures	Elements of software, firmware, hardware, or procedures that are included in the system for the satisfaction of security specifications [J].
security mode	See mode of operation. [J].

security officer	See system security officer, and information system security officer. [J].
security perimeter	Boundary where security controls are in effect to protect IS assets. [G].
security policy	The set of laws, rules, and practices that regulate how an organization manages, projects, and distributes sensitive or critical information. For example, a corporate security policy is the set of laws, rules, and practices within a user organization; system security policy defines the rules and practices within a specific system; and technical security policy regulates the use of hardware, software, and firmware of a system or product. [K].
security range	Highest and lowest security levels that are permitted in or on an IS, system component, subsystem, or network. [G].
security requirements	Types and levels of protection necessary for equipment, data, information, applications and facilities to meet security policy. [G].
security requirements baseline	Description of the minimum requirements necessary for an IS to maintain an acceptable level of security. [G].
security relevant event	Any event that attempts to change the security state of the system, (e.g., change discretionary access controls, change the security level of the subject, change user password, etc.). Also, any event that attempts violate the security policy of the system (e.g., too many attempts to login, attempts to violate the mandatory access control limits of a device, attempts to downgrade a file,etc.). [J].
security safeguards	Protective measures and controls that are prescribed to meet the security requirements specified for an IS. NOTE: Safeguards may include security features, as well as management constraints, personnel security, and security of physical structures, areas, and devices. (See accreditation.) [G].
security specification	Detailed description of the safeguards required to protect an IS. [G].
security target	A specification of the security required of a Target of Evaluation, used as a baseline for evaluation. The security target will specify the security enforcing functions of the

	Target of Evaluation. It will also specify the security objectives, the threats to those objectives, and any specific security mechanisms that will be employed. [J].
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. [G].
security testing	Process to determine that an IS's security features protects data and maintains functionality as intended. 22[G]. This may include hands-on functional testing, penetration testing, and verification. [J]. NOTE: Security testing may reveal vulnerabilities beyond the scope of the IS design. [G].
security threat	See threat. [J].
security top-level specification	See DTLS and FTLS. [J].
Security Working Group	A group, representing various organizational entities, that meets to discuss security issues throughout a system's life cycle. Note: Identification of security issues and suggested solutions are outputs of the group. [K].
seed key	Initial key used to start an updating or key generation process. [G].
selective routing	The ability to choose or avoid specific networks, links or relays. [J].
self-authentication	Implicit authentication, to a predetermined level, of all transmissions on a secure communications system. [G].
Sensitive Compartmented Information (SCI)	All Intelligence Information and material that requires special controls for restricted handling within compartmented channels and for which compartmentization is established. [J].
sensitive information	Information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under 5 U.S.C. Section 552a (the Privacy Act), but that has not been specifically

authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

NOTE: 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). [G].

sensitivity	Classification level plus caveats and handling restrictions. [I].
sensitivity label	<p>Piece of information that represents elements of the security label(s) of a subject and an object.</p> <p>NOTE: Sensitivity labels are used by the trusted computing base as the basis for mandatory access control decisions. [G].</p>
separation of duties	The specification and enforcement of user roles, and the allocation of responsibilities and privileges between these roles(e.g., operator, system administrator, security officer). This is a an essential requirement for the enforcement of the principle of least privilege. [J].
session security level	The security level associated with a process (session) that is used in the enforcement of mandatory access controls for the process. The session level defines the level of information that the process can access and it must be dominated by the clearance/authorization of the user on whose behalf the process is executing. [J].
Shielded Enclosure (SE)	Room or container designed to attenuate electromagnetic radiation. [G].
short title	<p>Identifying combination of letters and numbers assigned to certain COMSEC materials to facilitate handling, accounting, and control.</p> <p>NOTE: NAG-16C/TSEC is an example of a short title. [G].</p>
signals security	Generic term encompassing communications security and electronic security. [G].
simple security property	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. [G].8

single key encryption	Encryption algorithm where a single private key is used to both encrypt and decrypt information. [J].
single-level device	IS device that is not trusted to properly maintain and separate data to different security levels. [G].
single point keying	Means of distributing key to multiple, local crypto-equipment or devices from a single fill point. [G].
single trusted system	A network having an overall security architecture allowing its evaluation under Part I of the TNI and assignment of an evaluation class. Contrast with interconnected accredited (A)IS which are sufficiently complex and heterogeneous that no single evaluation rating can adequately reflect the trust placed in the network. [J].
smart card	A credit card size electronic computing device that, using an algorithm and secret key, can be used to authenticate a user to a system. [J].
software	Various programming aids that are frequently supplied by the manufacturers to facilitate the purchaser's efficient operation of the equipment. Such software items include various assemblers, generators, subroutine libraries, compilers, operating systems, and industry application programs.
software development methodologies	Methodologies for specifying and verifying design programs for system development. Each methodology is written for a specific computer language. See affirm, EHDM, FDM, Gypsy Verification Environment and HDM. [J].
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. [G].
special	The specification language used in the hierarchical development methodology. [J].
special access program	Any program which is established to control access, distribution, and to provide protection for particularly sensitive classified information beyond that normally required for Top Secret, Secret, or Confidential information. A Special Access Program can be created or continued only as authorized by the Head of a User

Agency who was delegated such authority in E.O. 12356. [J].

special mission modification

Modification that applies only to a specific mission, purpose, operational, or environmental need.

NOTE: Special mission modifications may be either optional or mandatory. [G].

speech privacy

Techniques that use fixed sequence permutations or voice/speech inversion to render speech unintelligible to the casual listener. [G].

spelling table

Synonymous with syllabary. [G].

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. [G].

spoofing

(COMSEC) Interception, alteration, and retransmission of a cipher signal or data in such a way as to mislead the recipient.

(IS) Attempt to gain access to an IS by posing as an authorized user. [G].

spread spectrum

Telecommunications techniques in which a signal is transmitted in a bandwidth considerably greater than the frequency content of the original information.

NOTE: Frequency hopping, direct sequence spread ing, time scrambling, and combinations of these techniques are forms of spread spectrum. [G].

stand-alone, shared system

A system that is physically and electrically isolated from all other systems, and is intended to be used by more than one person, either simultaneously (e.g., a system with multiple terminals) or serially, with data belonging to one user remaining available to the system while another user is using the system(e.g., a personal computer with nonremovable storage media such as hard disk). [J].

stand-alone, single-user system

A system that is physically and electrically isolated from all other systems, and is intended to be used by one person at a time, with no data belonging to other users remaining in the system (e.g., a personal computer with removable storage media such as a floppy disk). [J].

standard practice procedures	A document(s) prepared by a contractor and approved by the CSO that implements the applicable requirements of the ISM for the contractor's operations and involvement with classified information at the contractor's facility. [J].
star property	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. [G].
start-up KEK	Key encryption key held in common by a group of potential communicating entities and used to establish ad hoc tactical nets. [G].
State Delta Verification System (SDVS)	A system designed to give high confidence regarding microcode performance by using formulae that represent isolated states of a computation to check proofs concerning the course of that computation. [J].
state variable	Variable that represents either the state of an IS or the state of some system resource. [G].
storage object	Object that supports both read and write accesses to an IS. [G]
strength of mechanisms	An aspect of the assessment of the effectiveness of a Target of Evaluation, namely the ability of its security mechanisms to withstand direct attack against deficiencies in their underlying algorithms, principles and properties. [J].
strictly dominates	In comparing two security levels S1 and S2, when S1 dominates but is not equal to S2, then S1 is said to strictly dominate S2. [J].
STU-III	A Secure Telephone Unit using end-to-end encryption to provide secure voice and data communications. Type I STU-III units are Controlled Cryptographic Items(CCI) that can adequately protect all levels of classified information when appropriately keyed. [J].
structure of controls	The controls in and around the computer system that provide protection against the four threats (unauthorized modification, unauthorized disclosure, destruction, and denial of service). [H].

subassembly	Major subdivision of a cryptographic assembly which consists of a package of parts, elements, and circuits that performs a specific function. [G].
subject	Any active entity in the system (e.g., person, process (i.e., an executing program), or device) that causes information to flow among objects or changes the system state (e.g., from operating on the behalf of the system to operating on the behalf of the user). [H].
subject security level	Sensitivity label(s) of the objects to which the subject has both read and write access. NOTE: Security level of a subject must always be dominated by the clearance level of the user with which the subject is associated. [G].
subset-domain	A set of system domains. For evaluation by parts, each candidate TCB subset must occupy a distinct subset domain such that modifying access to a domain within a TCB subset's subset-domain is permitted only to that TCB subset and (possibly to more primitive TCB subset). [J].
subsystem	A secondary or subordinate system, usually capable of operating independently of, or asynchronously with, a controlling system.
superencryption	Process of encrypting encrypted information. NOTE: 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. [G].
supersession	Scheduled or unscheduled replacement of a COMSEC aid with a different edition. [G].
supervisor state	Synonymous with executive state. [G].
suppression measure	Action, procedure, modification, or device that reduces the level of, or inhibits the generation of, compromising emanations in a telecommunications or automated information system. [G].
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.

NOTE: A syllabary may also be known as a spelling table. [G].

symmetric encryption

See single key encryption. [J].

synchronous crypto-operation

Method of on-line crypto-operation in which crypto-equipment and associated terminals have timing systems to keep them in step. [G].

system

A process that may include computer hardware, software, data, procedures, and people, so related as to behave as an interacting or interdependent unity. A system has a particular purpose and operational environment. A system may contain one or more components or products. [L].

System Administrator (SA)

A role responsible for the maintenance of the non-security aspect of a system such as file system and user account maintenance, performance tuning, device management, and applications, tools, and operating system (non-TCB) installation and maintenance. See System Security Officer and Information System Security Officer. [J].

system development methodologies

Methodologies developed through software engineering to manage the complexity of system development.

NOTE: Development methodologies include software engineering aids and high-level design analysis tools. [G].

system high

Highest security level supported by an IS. [G].

System High (security) Mode

1. An IS is operating in the system high mode when all of its users possess the proper security clearance, but do not necessarily have a need-to-know for accessing all data processed and stored by the IS. ISs containing only unclassified information, as well as those containing both unclassified and classified information, can operate in the system high mode. All information is handled at the highest classification processed by the system. [H].

2. 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 non-disclosure agreements for all the information stored and/or processed (including all compartments, subcompartments and/or special access programs).
- c. Valid need-to-know for some of the information contained within the IS. [G].

system indicator	Symbol or group of symbols in an off line encrypted message that identifies the specific cryptosystem or key used in the encryption. [G].
system integrity	Quality of an IS when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system. [G].
system life cycle	The duration of time that begins with the identification of a need to place a system into operation; continues through the system's design, development, implementation and operation; and ends with the system's disposal. [K].
system low	Lowest security level supported by an IS. [G].
system security	Measure of security provided by a system, as determined by evaluation of the totality of all system elements and COMSEC measures that support telecommunications and IS protection. [G].
system security engineering	The efforts that help achieve maximum security and survivability of a system during its life cycle and interfacing with other program elements to ensure security functions are effectively integrated into the total system engineering effort. [G].
system security evaluation	Determination of the risk associated with the use of a given system, considering its vulnerabilities and perceived security threat. [G].
system security management plan	A formal document that fully describes the planned security tasks required to meet system security requirements. [G].
system security officer	Synonymous with information system security officer. [G].

T

tampering	Unauthorized modification that alters the proper functioning of a cryptographic or IS security equipment or system in a manner that degrades the security or functionality it provides. [G].
tape mixer	Teletypewriter security equipment that encrypts plain text and decrypts cipher text by combining them with a key stream from a one-time tape. [G].
TCB subset	A set of software, firmware, and hardware (where any of these three could be absent) that mediates the access of a set S of subjects to a set O of objects on the basis of a stated access control policy P and satisfies the properties: (1) M mediates every access to objects O by subjects in S; (2) M is tamper resistant; and (3) M is small enough to be subject to analysis and tests, the completeness of which can be assured. [J].
technical attack	Attack that can be perpetrated by circumventing or nullifying hardware or software protection mechanisms, rather than by subverting system personnel or other users. [G].
technical penetration	Deliberate penetration of a security area by technical means to gain unauthorized interception of information-bearing energy. [G].
Technical Point Of Contact (TPOC)	A person designated by the NSA during product evaluation and RAMP as the technical point of contact within the NSA to which all technical questions from a vendor with regard to their specific product should be directed. Each product is assigned a TPOC who is to be kept up to date on the status and progress of the product and used as a resource by vendors when they have questions about the evaluation of their product. [J].
Technical Review Board (TRB)	The panel of senior evaluators to which the evaluators present evidence during the NSA evaluation process. A TRB meets at the end of three different phases of the product evaluation process: DAP, Formal Evaluation Phase and RAMP. The TRB generates a recommendation at each stage. These recommendations fall into three categories: (1) pass, (2) pass with some exceptions, (3) fail. The actual outcome is decided by NSA management,

who use the TRB results as input into their decision process. The RAMP TRB is slightly different in that vendor personnel present to the TRB, rather than the government evaluators. [J].

technical security hazard Condition that could permit the technical penetration of an area through equipment that by reason of its normal design, installation, operation, maintenance, or damaged condition, allows the unauthorized transmission of classified information. [G].

technical security policy Specific protection conditions and/or protection philosophy that express the boundaries and responsibilities of the IT product or system in supporting the information protection policy control objectives and countering expected threats. [J].

technical security material Equipment, components, devices, and associated documentation or other media that pertains to cryptography or the securing of telecommunications and automated information systems. [G].

telecommunications Preparation, transmission, communication, or related processing of information (writing, images, sounds or other data) by electrical, electromagnetic, electro-mechanical, electro-optical or electronic means. [G].

telecommunications and automated information systems security Protection afforded to telecommunications and automated information systems, in order to prevent exploitation through interception, unauthorized electronic access, or related technical intelligence threats and to ensure Authenticity.

NOTE: Such protection results from the application of security measures (including cryptosecurity, transmission security, emission security, and computer security) to systems that generate, store, process, transfer, or communicate information of use to an adversary, and also includes the physical protection of technical security material and technical security information. [G].

telecommunications security Synonymous with communications security. [G].

TEMPEST Short name referring to investigation, study, and control of compromising emanations from telecommunications and automated information systems equipment. (See compromising emanations.) [G].

TEMPEST test	Laboratory or on-site test to determine the nature of compromising emanations associated with a telecommunications or automated information system. [G].
TEMPEST zone	Defined area within a facility where equipment with appropriate TEMPEST characteristics (TEMPEST zone assignment) may be operated without emanating electromagnetic radiation beyond the controlled space boundary of the facility. NOTE: Facility TEMPEST zones are determined by measuring electromagnetic attenuation provided by a building's properties and the free space loss to the controlled space boundary. Equipment TEMPEST zone assignments are based on the level of compromising emanations produced by the equipment. [G].
terminal identification	Means used to uniquely identify a terminal to an IS. [G].
test key	Key intended for on-the-air testing of COMSEC equipment or systems. [G].
testbed	A system representation consisting partially of actual hardware and/or software and partially of computer models or prototype hardware and/or software. [K].
threat	Capabilities, intentions, and attack methods of adversaries to exploit, or any circumstance or event with the potential to cause harm to, information or an information system. [G].
threat analysis	Process of studying information to identify the nature of and elements comprising a threat. [G].
threat assessment	Process of formally evaluating the degree of threat to an information system and describing the nature of the threat. [G].
threat monitoring	Analysis, assessment, and review of IS audit trails and other data collected for the purpose of searching out system events that may constitute violations or attempted violations of data or system security. [G].
ticket-oriented	Computer protection system in which each subject maintains a list of unforgeable bit patterns called tickets,

	one for each object that a subject is authorized to access. (See list-oriented.) [G].
tiger team	A testing strategy, typically used only after a system is felt to be very stable, in which a team of experts attempt to identify and exploit flaws in the system begin tested. [J].
time bomb	Logic bomb for which the logic trigger is time. [G].
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. [G].
time-dependent password	Password that is valid only at a certain time of day or during a specified interval of time. [G].
Top Secret (TS)	The designation that shall be applied only to information or material the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security. Examples of "exceptionally grave damage" include armed hostilities against the U.S. or its allies, disruption of foreign relations vitally affecting the national security, the compromise of vital national defense plans or complex cryptologic and communication intelligence systems, the revelation of sensitive intelligence operations, and the disclosure of scientific or technological development vital to national security. [J].
Top-Level Specifications (TLS)	A non-procedural description of system behavior at the most abstract level. Typically, a functional specification that omits all implementation details. See DTLS and FTLS. [J].
trace a correspondence	Explain a correspondence, using natural language prose, between levels of abstraction. [J].
traditional COMSEC program	COMSEC program in which the National Security Agency acts as the central procurement agency for the development and, in some cases, the production of COMSEC items. NOTE: This includes the Authorized Vendor Program and user partnerships. modifications to the COMSEC end items used in products developed and/or produced under these programs must be approved by the National Security Agency. [G].

traffic analysis	Study of communications characteristics external to the text. [G].
traffic encryption key	Key used to encrypt plain text or to superencrypt previously encrypted text and/or to decrypt cipher text. [G].
traffic-flow security	Measure used to conceal the presence of valid messages in an on-line cryptosystem or secure communications system. NOTE: Encryption of sending and receiving addresses and causing the circuit to appear busy at all times by sending dummy traffic are two methods of traffic-flow security. A more common method is to send a continuous encrypted signal, irrespective of whether traffic is being transmitted. [G].
traffic padding	Generation of spurious communications or data units to disguise the amount of real data units being sent. [G].
training key	Cryptographic key intended for on-the-air or off-the-air training. [G].
tranquility	Property whereby the security level of an object cannot change while the object is being processed by an IS. [G].
tranquility property	A security model rule stating that the security level of an active object cannot change during the period of activity. [J].
transmission security	Component of communications security that results from the application of measures designed to protect transmissions from interception and exploitation by means other than cryptanalysis. [G].
transmission security key	Key that is used in the control of transmission security processes, such as frequency hopping and spread spectrum. [G].
trap door	Hidden software or hardware mechanism that can be triggered to permit protection mechanisms in an IS to be circumvented. NOTE: A trap door is usually activated in some innocent-appearing manner; e.g., a special random key sequence at a terminal. Software developers often write trap doors in

their code that enable them to reenter the system to perform certain functions. [G].

Trojan horse

Computer program containing an apparent or actual useful function that contains additional (hidden) functions that allows unauthorized collection, falsification or destruction of data. [G].

trust

Confidence that an entity, to which trust is applied, will perform in a way that will not prejudice the security of the user of the system of which that entity is a part.

Note: Trust is always restricted to specific functions or ways of behavior (e.g., "trusted to connect A to B properly"). Trust is meaningful only in the context of a security policy; an entity may be trusted in the context of one policy, but untrusted in the context of another policy. [K].

trusted computer system

IS that employs sufficient hardware and software assurance measures to allow simultaneous processing of a range of classified or sensitive information. [G].

Trusted Computer System
Evaluation Criteria (TCSEC)

A document published by the National Computer Security Center containing a uniform set of basic requirements and evaluation classes for assessing degrees of assurance in the effectiveness of hardware and software security controls built into systems. These criteria are intended for use in the design and evaluation of systems that will process and/or store sensitive or classified data. This document is Government Standard DoD 5200.28-STD and is frequently referred to as "The Criteria" or "The Orange Book." [J].

trusted computing base (TCB)

Totality of protection mechanisms within a computer system, including hardware, firmware, and software, the combination of which is responsible for enforcing a security policy.

NOTE: The ability of a trusted computing base to enforce correctly a unified security policy depends on the correctness of the mechanisms within the trusted computing base, the protection of those mechanisms to ensure their correctness, and the correct input of parameters related to the security policy. [G].

Trusted Database Interpretation (TDI)	A document published by the NCSC interpreting the TCSEC for trusted applications in general and database management systems in particular. [J].
trusted distribution	Method for distributing trusted computing base hardware, software, and firmware components, both originals and updates, that provides protection of the trusted computing base from modification during distribution, and for the detection of any changes. [G].
trusted facility management	The administrative procedures, roles, functions (e.g., commands, programs, interfaces), privileges and databases that are used for secure system configuration, administration, and operation. [J].
Trusted Facility Manual (TFM)	A document necessary to satisfy the requirement of any TCSEC class. The TFM is directed towards administrators of an installation. It provides detailed information on how to: (1) configure and install the secure system; (2) operate the system securely; (3) correctly and effectively use system privileges and protection mechanisms to control access to administrative functions; and (4) avoid improper use of those functions which could compromise TCB and user security. [J].
trusted identification forwarding	<p>An identification method used in IS networks whereby the sending host can verify that an authorized user is attempting a connection to another host.</p> <p>NOTE: The sending host transmits the required user authentication information to the receiving host. The receiving host can then verify that the user is validated for access to the system. This operation may be transparent to the user. [G].</p>
Trusted Network Interpretation (TNI)	A document published by the NCSC interpreting the TCSEC for network product evaluations. This document is frequently referred to as "The Red Book". [J].
trusted path	<p>Mechanism by which a person using a terminal can communicate directly with the trusted computing base.</p> <p>NOTE: Trusted path can only be activated by the person or the trusted computing base and cannot be imitated by untrusted software. [G].</p>

trusted process	Process that has privileges to circumvent the system security policy and has been tested and verified to operate only as intended. [G].
Trusted Product Evaluation Program (TPEP)	The NSA program to evaluate trusted products developed to meet a level of assurance specified in the TCSEC. Evaluated products are placed on the evaluated products list (EPL) which is a part of the National Security Agency Information Systems Security Products and Services Catalogue. [J].
trusted products	Those products that have been specifically developed to enforce a security policy with some degree of assurance, such as those that have gone through the TPEP and were placed on the EPL. [J].
trusted recovery	The ability to ensure that recovery without a protection compromise can be accomplished after a system failure or other discontinuity. [J].
trusted software	Software portion of a trusted computing base. [G].
trusted subject	A subject that is permitted to have simultaneous view-and alter-access to objects of more than one sensitivity level. [J].
trusted system	A system that is trusted to enforce a specific security policy. [J].
TSEC nomenclature	System for identifying the type and purpose of certain items of COMSEC material. NOTE: TSEC is derived from telecommunications security. [G].
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. [G].
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. [G].

two-person integrity

System of storage and handling designed to prohibit individual access to certain COMSEC keying material, by requiring the presence of at least two authorized persons, each capable of detecting incorrect or unauthorized security procedures with respect to the task being performed.

NOTE: Two-person integrity procedures differ from no-lone zone procedures in that, under two-person integrity controls, two authorized persons must directly participate in the handling and safeguarding of the keying material (as in accessing storage containers, transportation, keying/rekeying operations, and destruction). No-lone zone controls are less restrictive in that the two authorized persons need only to be physically present in the common area where the material is located. Two person control refers to nuclear command and control COMSEC material while two person integrity refers only to COMSEC keying material. [G].

type 1 product

Classified or controlled cryptographic item endorsed by the National Security Agency for securing classified and sensitive U.S. Government information, when appropriately keyed.

NOTE: The term refers only to products, and not to information, key, services, or controls. Type 1 products contain classified National Security Agency 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. [G].

type 2 product

Unclassified cryptographic equipment, assembly, or component, endorsed by the National Security Agency, for use in telecommunications and automated information systems for the protection of national security information.

NOTE: The term refers only to products, and not to information, key, services, or controls. Type 2 products may not be used for classified information, but contain classified National Security Agency algorithms that distinguish them from products containing the unclassified data encryption standard algorithm. Type 2 products are

NAVSO P-5239-02
JUNE 1995

available to U.S. Government departments and agencies and sponsored elements of state and local governments, sponsored U.S. Government contractors, and sponsored private sector entities. Type 2 products are subject to export restrictions in accordance with the International Traffic in Arms Regulation. [G].

type 3 algorithm

Cryptographic algorithm that has been registered by the National Institute of Standards and Technology and has been published as a Federal Information Processing Standard for use in protecting unclassified sensitive information or commercial information. [G].

type 4 algorithm

Unclassified cryptographic algorithm that has been registered by the National Institute of Standards and Technology, but is not a Federal Information Processing Standard. [G].

type accreditation

Official authorization by the DAA to employ a system in a specified environment.

Note: Type accreditation includes a statement of residual risk, delineates the operating environment, and identifies specific use. It may be performed when multiple copies of a system are to be fielded in similar environments. [K].

U

unauthorized disclosure	The revelation of information to individuals not authorized to receive it. [G].
unclassified	Information that has not been determined, pursuant to E.O. 12356 or any predecessor order, to require protection against unauthorized disclosure and that is not designated as classified. [G].
unclassified but sensitive information	Any information the loss, misuse, or unauthorized access to, or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under the Privacy Act, but which has not been specifically authorized under criteria established by an Executive Order (OR) or an Act of Congress to be kept secret in the interest of national defense or foreign policy. [L].
untrusted process	Process that has not been tested and verified for adherence to the security policy. NOTE: Untrusted process may include incorrect or malicious code that attempts to circumvent the security mechanisms. [G].
updating	Automatic or manual cryptographic process that irreversibly modifies the state of a COMSEC key, equipment, device, or system. [G].
upgrade	This is a determination that certain classified information, in the interest of national security, requires a higher degree of protection against unauthorized disclosure than currently provided, coupled with a changing of the classification designation to reflect such a higher degree. See Regrade. [J].
user	Person or process accessing an IS by direct connections (e.g., via terminals) or indirect connections. NOTE: "Indirect connection" relates to persons who prepare input data or receive output that is not reviewed for content or classification by a responsible individual. [G].
user authentication	See Identification and Authentication. [J].

user ID	Unique symbol or character string that is used by an IS to uniquely identify a specific user. [G].
User Partnership Program	Partnership between the National Security Agency and a U.S. Government department or agency to facilitate the development of secure information processing and communications equipment incorporating National Security Agency approved cryptographic security. [G].
user profile	Patterns of a user's activity on an IS that can be used to detect changes in normal routines. [G].
user representative	Person authorized by an organization to order COMSEC keying material and to interface with the keying system to provide information to key users, ensuring that the correct type of key is ordered. [G].
user state	A hardware execution state not permitting the use of privileged instructions. [J].
U.S. controlled facility	Base or building, access to which is physically controlled by U.S. persons who are authorized U.S. Government or U.S. Government contractor employees. [G].
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. persons who are authorized U.S. Government or U.S. Government contractor employees. NOTE: Keys or combinations to locks controlling entrance to U.S. controlled spaces must be under the exclusive control of U.S. persons who are U.S. Government or U.S. Government contractor employees. [G].
U.S. person	United States citizen or resident alien. [G].

V

valid password	A personal password that will authenticate the identity of an individual when presented to a password system or an access password that will allow the requested access when presented to a password system. [J].
validation	<p>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.</p> <p>NOTE: This action will include, as necessary, final development, evaluation, and testing, preparatory to acceptance by senior security test and evaluation staff specialists. [G].</p>
variant	One of two or more code symbols which have the same plain text equivalent. [G].
Vendor Assistance Phase (VAP)	The second phase of the NSA evaluation process where the NSA helps the vendor understand the TCSEC requirements as they pertain to that vendor's product and its desired evaluation class. The vendor applies this knowledge to the development of its product. [J].
Vendor Security Analyst (VSA)	A member of a vendor's staff that is recognized by the NSA, by virtue of completing the NSA VSA training course, as competent to represent that vendor's product to the NSA during RAMP. This entails participating in the security analysis process of the product being maintained and presenting the RAMP evidence to the TRB at the end of a RAMP cycle. [J].
verification	<p>The 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).</p> <p>NOTE: This process may or may not be automated. [G].</p>
verified design	Computer protection class in which formal security verification methods are used to assure that the IS mandatory and discretionary security controls can effectively protect classified and sensitive information stored in, or processed by, the system.

NOTE: Class A1 system is verified design. [G].

view	That portion of the database that satisfies the conditions specified in a query. [J].
view definition	A stored query; sometimes loosely referred to as a "view". [J].
virtual password	IS password computed from a passphrase that meets the requirements of password storage (e.g., 64 bits). [G].
virus	Self replicating, malicious program segment that attaches itself to an application program or other executable system component and leaves no external signs of its presence. [G].
vulnerability	Weakness in an information system, or cryptographic system, or components (e.g., system security procedures, hardware design, internal controls) that could be exploited [G] to violate system security policy.
vulnerability analysis	Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation. [G].
vulnerability assessment	A measurement of vulnerability which includes the susceptibility of a particular system to a specific attack and the opportunities available to a threat agent to mount that attack. [J].

W

waiver	With respect to C&A, a waiver implies that a security requirement has been set aside and need not be implemented at all. (See Exception.) [K].
wiretapping	The interception of messages (passive wiretapping), and the deliberate modifications made to a message stream (active wiretapping). [J].
work factor	Estimate of the effort or time needed by a potential perpetrator, with specified expertise and resources, to overcome a protective measure. NOTE: In cryptography, a work factor is the number of computer binary operations needed to guarantee that a particular key will not be recovered through cryptanalysis. [G].
worm	Independent program that replicates from machine to machine across network connections often clogging networks and computer systems as it spreads. [G].
write	Fundamental operation in an IS that results only in the flow of information from a subject to an object. (See access type.) [G].
write access	Permission to write to an object in an IS. [G].
write down	Occurs when a subject with access to high level data transfers that data to a lower level object. The Star Property of the Bell-Lapadula model prohibits this. [J].

Y

Yellow Book

Alternate name for DoD manual CSC-STD-003-85 originating from its yellow cover. This manual provides guidance for applying the TCSEC to specific environments. [J].

Z

zeroize

Remove or eliminate the key from a crypto-equipment or fill device. [G].

SECTION II

COMMONLY USED ABBREVIATIONS AND ACRONYMS

ACL	access control list
ADM	advanced development model
ADP	automated data processing
AE	application entity
AIG	address indicator group
AIRK	area interswitch rekeying key
AJ	anti-jamming
AK	automatic remote rekeying
AKDC	automatic key distribution center
AKD/RCU	automatic key distribution/rekeying control unit
AKM	automated key management center
ALC	accounting legend code
AMS	1. auto-manual system 2. autonomous message switch
ANDVT	advanced narrowband digital voice terminal
ANSI	American National Standards Institute
AOSS	automated office support systems
APC	adaptive predictive coding

APU	auxiliary power unit
ARPANET	Advanced Research Projects Agency Network
ASCII	American standard code for information interchange
ASPJ	advanced self-protection jammer
ASU	approval for service use
AUTODIN	Automatic Digital Network
AV	auxiliary vector
AVP	Authorized Vendor Program
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
CAP	Controlled Access Protection
CCEP	Commercial COMSEC Endorsement Program
CCI	controlled cryptographic item
CCO	circuit control officer
CDS	cryptographic device services
CEOI	communications electronics operation instruction

CEPR	compromising emanation performance requirement
CERT	computer emergency response team
CFD	common fill device
CIAC	computer incident assessment capability
CIK	crypto-ignition key
CIP	crypto-ignition plug
CIRK	common interswitch rekeying key
CK	compartment key
CKG	cooperative key generation
CLMD	COMSEC local management device
CMCS	COMSEC material control system
CNCS	cryptonet control station
CNK	cryptonet key
COMPUSEC	computer security
COMSEC	communications security
COR	central office of record
CPS	COMSEC parent switch
CPU	central processing unit
CRP	COMSEC resources program (Budget)
Crypt/Crypto	cryptographic-related
CSE	communications security element

CSS	<ol style="list-style-type: none">1. COMSEC subordinate switch2. Constant Surveillance Service (courier)3. Continuous Signature Service (Courier)4. coded switch system
CSSO	computer special security officer
CSTVRP	Computer Security Technical Vulnerability Reporting Program
CTAK	cipher text auto-key
CTTA	certified TEMPEST technical authority
CUP	COMSEC Utility Program
DAA	designated approving authority
DAC	discretionary access control
DAMA	demand assigned multiple access
DCS	<ol style="list-style-type: none">1. Defense Communications System2. Defense Courier Service
DCSP	design controlled spare part(s)
DDN	Defense Data Network
DDS	dual driver service (courier)
DES	data encryption standard
DIB	directory information base
DoD TCSEC	Department of Defense Trusted Computer System Evaluation Criteria

DLED	dedicated loop encryption device
DMA	direct memory access
DPL	Degausser Products List (a section in the Information Systems Security Products and Services Catalogue)
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 emergency action message
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
EDESPL	Endorsed Data Encryption Standard Products List
EDM	engineering development model
EFD	electronic fill device
EFTO	encrypt for transmission only
EGADS	Electronic Generation, Accounting, and Distribution System
EKMS	Electronic Key management System

ELINT	electronic intelligence
ELSEC	electronic security
E Model	engineering development model
EMSEC	emission security
EPL	Evaluated Products List (a section in the Information Systems Security Products and Services Catalogue)
ERTZ	equipment radiation TEMPEST zone
ETL	Endorsed Tools List
ETPL	Endorsed TEMPEST Products List item
EUCI	endorsed for unclassified cryptographic information
EV	enforcement vector
FDIU	fill device interface unit
FIPS	Federal Information Processing Standards
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
GPS	Global Positioning System

GTS	Global Telecommunications Service
GWEN	Ground Wave Emergency Network
HDM	Hierarchical development methodology
HMS	human safety mandatory modification
HUS	hardened unique storage
HUSK	hardened unique storage key
IATO	Interim Authority To Operate
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
IIRK	interarea interswitch rekeying key
ILS	integrated logistics support
INFOSEC	information systems security
IP	internet protocol
IPM	interpersonal messaging
IPSO	internet protocol security option
IR	information ratio
IRK	interswitch rekeying key

IS	information system
ISDN	Integrated Services Digital Network
ISO	International Standards organization
ISS	information systems security
ISSM	Information Systems Security Manager
ISSO	Information Systems Security Officer
ITAR	International Traffic in Arms Regulation
JTIDS	Joint Tactical Information Distribution System
KAK	key-auto-key
KEK	key encryption key
KMASE	key management application service element
KMC	key management center
KMID	key management identification number
KMODC	key material ordering and distribution center
KMP	key management protocol
KMPDU	key management protocol data unit
KMS	key management system
KMSA	key management system agent
KMUA	key management user agent
KP	key processor
KPK	key production key

KVG	key variable generator
KG	key generator
LAN	local area network
LCM	Life Cycle Management
LEAD	low-cost encryption/authentication device
LKG	loop key generator
LMD	local management device
LME	layer management entry
LMI	layer management interface
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	mandatory modification
MATSYM	material symbol
MCCB	modification/configuration control board
MDC	manipulation detection code

MEECN	Minimum Essential Emergency Communications Network
MEP	management engineering plan
MER	minimum essential requirements
MES	message handling system
MI	message indicator
MIB	management information base
MIJI	meaconing, intrusion, jamming and interference
MINTERM	miniature terminal
MIPR	military interdepartmental purchase request
MLS	multilevel security
MOA	memorandum of agreement
MOU	memorandum of understanding
MRK	manual remote rekeying
MRT	miniature receiver terminal
MSE	mobile subscriber equipment
NACAM	National COMSEC Advisory Memorandum
NACSEM	National COMSEC Emanations Memorandum
NACSI	National COMSEC Instruction
NACSIM	National COMSEC Information Memorandum
NAK	negative acknowledge
NATO	North Atlantic Treaty Organization

NCCD	nuclear command and control document
NCS	1. National Communications System 2. National Cryptologic School 3. net control station
NCSC	National Computer Security Center
NETS	Nationwide Emergency Telecommunications Service
NETSEC	Network Security
NISAC	National Industrial Security Advisory Committee
NIST	National Institute of Standards and Technology
NLZ	no-lone zone
NSAD	network security architecture and design
NSD	National Security Directive
NSDD	National Security Decision Directive
NSEP	National Security Emergency Preparedness
NSO	network security officer
NSTAC	National Security Telecommunications Advisory Committee
NSTISSAM	National Security Telecommunications and Information Systems Security Advisory/Information Memorandum
NSTISSC	National Security Telecommunications and Information Systems Security Committee
NSTISSD	National Security Telecommunications and Information Systems Security Directive

NSTISSI	National Security Telecommunications and Information Systems Security Instruction
NSTISSP	National Security Telecommunications and Information Systems Security Policy
NTCB	network trusted computing base
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
OPT	optional modification
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	peer access approval

PAE	peer access enforcement
PAL	permissive action link
PC	personal computer
PCZ	protected communications zone
PDR	preliminary design review
PDS	protected distribution system
PDU	protocol data unit
PES	positive enable system
PKA	public key algorithm
PKC	public key cryptography
PKSD	programmable key storage device
P model	preproduction model
PLSDU	physical layer service data unit
PNEK	post-nuclear event key
PPL	Preferred Products List (a section in the Information Systems Security Products and Services Catalogue.)
PRBAC	partition rule base access control
PROM	programmable read-only memory
PROPIN	proprietary information
PSDU	physical layer service data unit
PSL	Protected Services List

PTT	push-to-talk
PWA	printed wiring assembly
PWDS	protected wireline distribution system
RAC	repair action
RACE	rapid automatic cryptographic equipment
RAM	random access memory
ROM	read-only memory
RQT	reliability qualification tests
SAMS	semiautomatic message switch
SAO	special access office
SAP	1. system acquisition plan 2. special access program
SARK	SAVILLE advanced remote keying
SCI	sensitive compartmented information
SCIF	sensitive compartmented information facility
SDNRIU	secure digital net radio interface unit
SDNS	Secure Data Network System
SDR	system design review
SFA	security fault analysis
SI	special intelligence
SIGSEC	signals security

SISS	Subcommittee on Information Systems Security of the NSTISSC
SMM	special mission mandatory modification
SMO	special mission optional modification
SMU	secure mobile unit
SPK	single point key(ing)
SPS	scratch pad store
SRR	security requirements review
SSO	special security officer
ST&E	security test and evaluation
STS	Subcommittee on Telecommunications Security of the NSTISSC
STU	secure telephone unit
TA	traffic analysis
TACTED	tactical trunk encryption device
TACTERM	tactical terminal
TAG	TEMPEST Advisory Group
TISS	telecommunications and automated information systems security
TCB	trusted computing base
TCD	time compliance data
TCSEC	DoD Trusted Computer System Evaluation Criteria

TD	transfer device
TED	trunk encryption device
TEK	traffic encryption key
TEP	TEMPEST Endorsement Program
TFM	trusted facility manual
TFS	traffic flow security
TLS	top-level specification
TNI	trusted network interpretation
TNIEG	trusted network interpretation environment guideline
TPC	two-person control
TPI	two-person integrity
TRANSEC	transmission security
TRB	technical review board
TRI-TAC	Tri-service Tactical Communications System
TSCM	technical surveillance countermeasures
TSEC	telecommunications security
TSK	transmission security key
UA	user agent
UIRK	unique interswitch rekeying key
UIS	user interface system
UPP	User Partnership Program

USDE	undesired signal data emanations
V model	advanced development model
VST	VINSON subscriber terminal
VTT	VINSON trunk terminal
WAN	wide area network
WWMCCS	Worldwide Military Command and Control System
XDM/X Model	experimental development model/exploratory development model

SECTION III

REFERENCES

- A. National Security Directive 42, dated 5 July 1990.
- B. Executive Order 12356, National Security Information, dated 6, April 1982.
- C. Executive Order 12333, United States Intelligence Activities, dated 4 December 1981.
- D. Public Law 100-235, Computer Security Act of 1987, dated 8 January 1988.
- E. 10 United States Code Section 2315, The Warner Amendment, dated 1 December 1981.
- F. 44 United States Code Section 3502(2), Public Law 96-511, Paperwork Reduction Act of 1980, dated 11 December 1980.
- G. NSTISSI No. 4009, National Information Systems Security (INFOSEC) Glossary, dated 5 June 1992.
- H. NAVSO P-5239-15, Naval Information Systems Management Center, Controlled Access Protection (CAP) Guidebook, DON CAP Awareness Video Script, dated January 1995.
- I. NAVSO P-5239-26, Naval Information Systems Management Center, Remanence Security Guidebook, dated September 1993.
- J. INFOSEC Handbook, ARCA, An Information Systems Security Reference Guide, dated 1993.
- K. NCSC-TG-029 ver. 1, National Computer Security Center, Introduction to Certification and Accreditation, dated January 1994.
- L. Introduction to Certification and Accreditation Concepts, MITRE Corp., June 1992.
- M. Information System Security Plan for SNAP III, SPAWAR, June 1993.

NAVSO P-5239-02
JUNE 1995

THIS PAGE INTENTIONALLY BLANK