

# Glossary

---

**\*-property (star property):** A Bell-LaPadula security model rule allowing a subject write access to an object only if the security level of the subject is dominated by the security level of the object. Also known as the confinement property.

## A

**acceptance inspection:** The final inspection to determine whether a facility or system meets the specified technical and performance standards. Note: This inspection is held immediately after facility and software testing and is the basis for commissioning or accepting the information system.

**acceptance procedure:** A procedure which takes objects produced during the development, production, and maintenance processes for a target of evaluation and, as a positive act, places them under the controls of a configuration control system.

**access:** (1) The ability and means to communicate with (that is, input to or receive output from) or otherwise make use of any information, resource, or component in an information technology (IT) product. (2) A specific type of interaction between a subject and an object that results in the flow of information from one to the other. Note: An individual does not have “access” if the proper authority or a physical, technical, or procedural measure prevents him or her from obtaining knowledge or having an opportunity to alter information, material, resources, or components.

**access control:** (1) The process of limiting access to the resources of an information technology (IT) product only to authorized users, programs, processes, systems (in a network), or other IT products. (Synonymous with controlled access and limited access.) (2) The limiting of rights or capabilities of a subject to communicate with other subjects, or to use functions or services in a computer system or network. (3) Restrictions controlling a subject’s access to an object.

**access control list:** (1) A mechanism implementing discretionary access control in an IT (information technology) product that identifies the users

who may access an object and the type of access to the object that a user is permitted. (2) A list of subjects authorized for specific access to an object. (3) A list of entities, together with their access rights, which are authorized to have access to a resource.

**access control mechanism:** (1) Security safeguards designed to detect and prevent unauthorized access, and to permit authorized access in an IT (information technology) product. (2) Hardware or software features, operating procedures, management procedures, and various combinations of these designed to detect and prevent unauthorized access and to permit authorized access in an automated system.

**access level:** The hierarchical portion of the security level used to identify the sensitivity of data and the clearance or authorization of users. Note: The access level, in conjunction with the nonhierarchical categories, forms the sensitivity label of an object. (See category, security level, and sensitivity label.)

**access list:** Synonymous with access control list.

**access mediation:** Process of monitoring and controlling access to the resources of an IT (information technology) product, including but not limited to the monitoring and updating of policy attributes during accesses as well as the protection of unauthorized or inappropriate accesses (see access control).

**access period:** A segment of time, generally expressed on a daily or weekly basis, during which access rights prevail.

**access port:** A logical or physical identifier that a computer uses to distinguish different terminal input/output data streams.

**access type:** The nature of an access right to a particular device, program, or file (for example, read, write, execute, append, modify, delete, or create).

**accountability:** (1) Means of linking individuals to their interactions with an IT (information technology) product, thereby supporting identification of and recovery from unexpected or unavoidable failures of the control objectives. (2) The quality or state that enables actions on an ADP (automated data processing) system to be traced to individuals who may then be held responsible. These actions include violations and attempted violations of the security policy, as well as allowed actions. (3) The property that enables activities on a system to be traced to individuals who may then be held responsible for their actions.

**accreditation:** (1) The procedure for accepting an IT (information technology) system to process sensitive information within a particular operational environment. (2) The formal procedure for recognizing both the technical competence and the impartiality of an IT test laboratory (evaluation body) to carry out its associated tasks. (3) Formal declaration by a designated approving authority that an automated information system (AIS) is approved to operate in a particular security configuration using a prescribed set of safeguards. (4) The managerial authorization and approval granted to an ADP (automated data processing) system or network to process sensitive data in an operational environment, made on the basis of a certification by designated technical personnel of the extent to which design and implementation of the system meet pre-specified technical requirements, for example, TCSEC (Trusted Computer System Evaluation Criteria), for achieving adequate data security. Management can accredit a system to operate at a higher or lower level than the risk level recommended (for example, by the requirements guideline) for the certification level of the system. If management accredits the system to operate at a higher level than is appropriate for the certification level, management is accepting the additional risk incurred. (5) A formal declaration by the DAA (designated approving authority) that the AIS (automated information system) is approved to operate in a particular security mode using a prescribed set of safeguards. Accreditation is the official management authorization for operation of an AIS and is based on the certification process as well as other management considerations. The accreditation statement affixes security responsibility with the DAA and shows that due care has been taken for security.

**accreditation authority:** Synonymous with designated approving authority.

**accreditation range:** The accreditation range of a host with respect to a particular network is a set of mandatory access control levels (according to "Computer Security Requirements: Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments," CSC-STD-003-85) for data storage, processing, and transmission. The accreditation range will generally reflect the sensitivity levels of data that the 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 use 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.

**add-on security:** The retrofitting of protection mechanisms, implemented by hardware or software.

**administration documentation:** The information about a target of evaluation supplied by the developer for use by an administrator.

**administrative security:** The management constraints and supplemental controls established to provide an acceptable level of protection for data. (Synonymous with procedural security.)

**administrator:** A person in contact with the target of evaluation who is responsible for maintaining its operational capability.

**algorithm:** A mathematical procedure that can usually be explicitly encoded in a set of computer language instructions that manipulate data. Cryptographic algorithms are mathematical procedures used for such purposes as encrypting and decrypting messages and signing documents digitally.

**application program interface:** System access point or library function that has a well-defined syntax and is accessible from application programs or user code to provide well-defined functionality.

**approval/accreditation:** The official authorization that is granted to an ADP (automated data processing) system to process sensitive information in its operational environment, based upon comprehensive security evaluation of the system's hardware, firmware, and software security design, configuration, and implementation, and of the other system procedural, administrative, physical, TEMPEST, personnel, and communications security controls.

**architectural design:** A phase of the development process wherein the top-level definition and design of a target of evaluation are specified.

**assignment:** Requirement in a protection profile taken directly as stated, without change, from the list of components or derived by placing a bound on a threshold definition. Note: The assignment of environment-specific requirements to generic component requirements is performed when a component requirement corresponds to an environment-specific requirement.

**assurance:** See profile assurance and development and evaluation assurance. (1) The degree of confidence that a target of evaluation adequately fulfills the security requirements. (2) A measure of confidence that the security features and architecture of an AIS accurately mediate and enforce the security policy. Note: The two main aspects of assurance are *effectiveness* and *correctness* (ITSEC — Information Technology Security Evaluation Criteria) or *development* and *evaluation* assurance (Federal Criteria).

**assurance level:** In evaluation criteria, a specific level on a hierarchical scale representing successively increased confidence that a target of evaluation adequately fulfills the security requirements.

**assurance profile:** An assurance requirement for a TOE (target of evaluation) whereby different levels of confidence are required in different security-enforcing functions.

**attack:** The act of trying to bypass security controls on a system. An attack may be active, resulting in the alteration of data; or passive, resulting in the release of data. Note: The fact that an attack is made does not necessarily mean that it will succeed. The degree of success depends on the vulnerability of the system or activity and the effectiveness of existing countermeasures.

**audit:** Independent review and examination of records and activities to determine compliance with established usage policies and to detect possible inadequacies in product technical security policies of their enforcement.

**audit trail:** (1) A set of records that collectively provide documentary evidence of processing used to aid in tracing from original transactions forward to related records and reports, and/or backward from records and reports to their component source transactions. (2) A chronological record of system activities that is sufficient to enable the reconstruction, reviewing, and examination of the sequence of environments and activities surrounding or leading to an operation, a procedure, or an event in a transaction from its inception to final results. (3) Information collected or used to facilitate a security audit. Note: Audit trail may apply to information in an IT (information technology) product or an AIS (automated information system) or to the transfer of COMSEC (communications security) material.

**authenticate:** (1) To verify the identity of a user, user device, or other entity, or the integrity of data stored, transmitted, or otherwise exposed to unauthorized modification in an IT (information technology) product. (2) To verify the validity of a claimed identity of a user, device, or other entity in a computer system, often as a prerequisite to allowing access to resources in a system. (3) To verify the integrity of data that have been stored, transmitted, or otherwise exposed to possible unauthorized modification.

**authentication:** (1) To establish the validity of a claimed identity. (2) To provide protection against fraudulent transactions by establishing the validity of a message, station, individual, or originator. (3) Means of veri-

ifying an entity's (for example, individual user's, machine's, or software component's) eligibility to receive specific categories of information.

**authenticator:** The means used to confirm the identity or to verify the eligibility of a station, originator, or individual.

**authorization:** Access rights granted to a user, program, or process.

**authorized:** Entitled to a specific mode of access.

**automated data processing (ADP) security:** Synonymous with automated information systems security.

**automated data processing (ADP) system:** An assembly of computer hardware, firmware, and software configured for the purpose of classifying, sorting, calculating, computing, summarizing, transmitting and receiving, storing, and retrieving data, with a minimum of human intervention.

**automated information system (AIS):** (1) Any equipment or interconnected systems or subsystems of equipment that are used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data and include computer software, firmware, and hardware. (2) An assembly of computer hardware, software, and/or automated information system (AIS) firmware configured to collect, create, communicate, compute, disseminate, process, store, and/or control data or information. Note: Included are computers, word processing systems, networks or other electronic information handling systems, and associated equipment.

**automated information systems (AIS) security:** Measures and controls that protect an AIS against denial of service and unauthorized (accidental or intentional) disclosure, modification, or destruction of AISs and data. AIS 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, remote computer, and terminal facilities; management constraints; physical structures and devices; and personnel and communication controls needed to provide an acceptable level of risk for the AIS and for the data and information contained in the AIS. It includes the totality of security safeguards needed to provide an acceptable protection level for an AIS and for data handled by an AIS.

**automated security monitoring:** The use of automated procedures to ensure that security controls are not circumvented.

**availability:** (1) The ability to access a specific resource within a specific time frame as defined within the IT (information technology) product specification. (2) The ability to use or access objects and resources as required. The property relates to the concern that information objects and other system resources are accessible when needed and without undue delay. (3) The prevention of the unauthorized withholding of information or resources.

## B

**back door:** Synonymous with trap door.

**backup plan:** Synonymous with contingency plan.

**bandwidth:** (1) A characteristic of a communication 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. (2) Rate at which information is transmitted through a channel. (See channel capacity.) Note: Bandwidth was originally a term used in analog communication, measured in hertz, and related to the information rate by the “sampling theorem” (generally attributed to H. Nyquist, although the theorem was in fact known before Nyquist used it in communication theory). Nyquist’s sampling theorem says that the information rate in bits (samples) per second is at most twice the bandwidth in hertz of an analog signal created from a square wave. In a covert-channel context, “bandwidth” is given in bits per second rather than hertz and is commonly used, in a nonstandard use of terminology, as a synonym for information rate.

**basic component:** A component that is identifiable at the lowest hierarchical level of a specification produced during detailed design.

**Bell-LaPadula model:** (1) A formal state-transition model of computer security policy that describes a set of access control rules. In this formal model, the entities in a computer system are divided into abstract sets of subjects and objects. The notion of a secure state is defined, and it is proven that each state transition preserves security by moving from secure state to secure state, thereby inductively proving that the system is secure. A system state is defined to be “secure” if the only permitted access modes of subjects to objects are in accordance with a specific security policy. To determine whether a specific access mode is allowed, the clearance of a subject is compared with the classification of the object, and a determination is made as to whether the subject is authorized for the specific access mode. The clearance/classifications scheme is expressed in terms of a lattice. (See \*-property (star property), simple security property, and lattice). (2) A formal state-transition model of a technical se-

curity policy for an AIS (automated information system) that presents: (a) access constraints (including initial-state constraints and variants or the simple security and star properties), (b) allowed state transitions (called “rules of operation”), and (c) a proof that the allowed state transitions guarantee satisfaction of the constraints.

**benign environment:** A nonhostile environment that may be protected from external hostile elements by physical, personnel, and procedural security countermeasures.

**between-the-lines entry:** Unauthorized access obtained by tapping the temporarily inactive terminal of a legitimate user. (See piggyback.)

**beyond A1:** A level of trust defined by the US DoD (Department of Defense) Trusted Computer System Evaluation Criteria (TCSEC) that is beyond the state-of-the-art technology available at the time the criteria were developed. It includes all the A1-level features plus additional ones not required at the A1 level.

**binding of security functionality:** The ability of security-enforcing functions and mechanisms to work together in a way that is mutually supportive and provides an integrated and effective whole.

**bit:** Short for binary digit — 0 or 1. Keys are strings of bits.

**browsing:** The act of searching through storage to locate or acquire information without necessarily knowing of the existence or the format of the information being sought.

## C

**call back:** A procedure for identifying a remote terminal. In a call back, the host system disconnects the caller and then dials the authorized telephone number of the remote terminal to reestablish the connection. (Synonymous with dial back.)

**Canadian Trusted Computer Product Evaluation Criteria (CTCPEC):** Canadian secure products criteria.

**candidate TCB (trusted computing base) 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 by parts.



**capability:** A protected identifier that both identifies the object and specifies the access rights to be allowed to the accessor who possesses the capability. In a capability-based system, access to protected objects such as files is granted if the would-be accessor possesses a capability for the object.

**category:** (1) A grouping of objects to which a nonhierarchical restrictive label is applied (for example, proprietary, compartmented information). Subjects must be privileged to access a category. (2) 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. Note: Examples include sensitive compartmented information and proprietary information. Individuals are granted access to a special category of information only after being granted formal access authorization.

**cellular transmission:** Data transmission via interchangeable wireless (radio) communications in a network of numerous small geographic cells. Most current technology is analog — represented as electrical levels, not bits. However, the trend is toward digital cellular data transmission.

**certification:** (1) Comprehensive evaluation of the technical and nontechnical security features of an AIS (automated information system) and other safeguards, made in support of the approval/accreditation process, to establish the extent to which a particular design and implementation meet a set of specified security requirements. Note: There remain two other definitions in active common usage that differ according to circumstances. (See IT (information technology) security certification and site certification.) (2) The issue of a formal statement confirming the results of an evaluation, and that the evaluation criteria used were correctly applied. Synonym for IT (information technology) security certification.

**certification body:** An independent and impartial national organization that performs certification. Also referred to as an evaluation body or entity.

**channel:** An information transfer path within a system — may also refer to the mechanism by which the path is effected.

**channel capacity:** Maximum possible error-free rate, measured in bits per second, at which information can be sent along a communications path.

**cleartext:** Intelligible data, the semantic content of which is available. Also referred to as plaintext.

**closed security environment:** An environment in which both of the following conditions hold true: (1) Application developers (including maintainers) have sufficient clearances and authorizations to provide an acceptable presumption that they have not introduced malicious logic and (2) configuration control provides sufficient assurance that applications and the equipment are protected against the introduction of malicious logic prior to and during the operation of system applications.

**closed user group:** A closed user group permits users belonging to a group to communicate with each other, but precludes communications with other users who are not members of the group.

**Common Criteria for Information Technology Security (CC):** Evolving international security evaluation criteria being developed by the US, Canada, the UK, Germany, and France.

**communication channel:** The physical media and devices that provide the means for transmitting information from one component of a network to (one or more) other components.

**communication link:** The physical means of connecting one location to another for the purpose of transmitting and/or receiving data.

**communications security (COMSEC):** Measures taken to deny unauthorized persons information derived from telecommunications of an entity concerning national or organizational security, and to ensure the authenticity of such telecommunications. Communications security includes cryptosecurity, transmission security, emission security, and physical security of communications security material and information.

**compartment:** (1) A designation applied to a type of sensitive information, indicating the special handling procedures to be used for the information and the general class of people who may have access to the information. It can refer to the designation of information belonging to one or more categories. (2) A class of information in the US government that has need-to-know access controls beyond those normally provided for access to Confidential, Secret, or Top Secret information.

**compartmented mode or compartmented security mode:** See modes of operation.

**component:** (1) A device or set of devices consisting of hardware, along with its firmware and/or software, that performs a specific function on a computer communications network. A component is a part of the larger system and may itself consist of other components. Examples include

modems, telecommunications controllers, message switches, technical control devices, host computers, gateways, communications subnets, and so on. (2) An identifiable and self-contained portion of a target of evaluation which is subjected to security evaluation. (3) An organization that is part of a larger organization, for example, a US Defense Component. (4) A requirement that is part of a larger set of requirements that may be called a package. For example, protection profiles are assembled from components. Groups of components can be assembled into predefined packages.

**component reference monitor:** An access control concept that refers to an abstract machine that mediates all access to objects within a component by subjects within the component.

**compromise:** A violation of the security system such that an unauthorized disclosure of sensitive information may have occurred.

**compromising emanations:** Unintentional data-related or intelligence-bearing signals that, if intercepted and analyzed, disclose the information transmission received, handled, or otherwise processed by any information processing equipment. (See TEMPEST.)

**computer abuse:** The misuse, alteration, disruption, or destruction of data processing resources. The key aspect is that it is intentional and improper.

**computer 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 computer system. Computer architecture features can be available to application programs and system programmers in several modes, including a protected mode. For example, the system-level features of computer architecture may include: (1) memory management, (2) protection, (3) multitasking, (4) input/output, (5) exceptions and multiprocessing, (6) initialization, (7) coprocessing and multiprocessing, (8) debugging, and (9) cache management.

**computer cryptography:** The use of a cryptoalgorithm in a computer, microprocessor, or microcomputer to perform encryption or decryption in order to protect information or to authenticate users, sources, or information.

**computer fraud:** Computer-related crimes involving deliberate misrepresentation, alteration, or disclosure of data to obtain something of value (usually for monetary gain). A computer system must have been involved in the perpetration or cover-up of the act or series of acts. A computer

system might have been involved through improper manipulation of input data, output or results, applications programs, data files, computer operations, communications, or computer hardware, systems software, or firmware.

**computer security (COMPUSEC) :** Synonymous with automated information systems (AIS) security.

**computer security subsystem:** A device designed to provide limited computer security features in a larger system environment.

**Computer Security Technical Vulnerability Reporting Program (CSTVRP):** A program that focuses on technical vulnerabilities in commercially available hardware, firmware, and software products acquired by the US Department of Defense. CSTVRP provides for the reporting, cataloging, and discreet dissemination of technical vulnerability and corrective measure information to Defense Components on a need-to-know basis.

**concealment system:** A method of achieving confidentiality in which sensitive information is hidden by embedding it in irrelevant data.

**confidentiality:** (1) The assurance that information is not disclosed to inappropriate entities or processes. (2) The property that information is not made available or disclosed to unauthorized entities. (3) The prevention of the unauthorized disclosure of information. (4) The concept of holding sensitive data in confidence, limited to an appropriate set of individuals or organizations.

**configuration:** Selection of one of the sets of possible combinations of features of a system or target of evaluation.

**configuration control:** (1) A system of controls imposed on changing controlled objects produced during the development, production and maintenance processes for a target of evaluation. (2) Management of changes made to a system's hardware, software, firmware, and documentation throughout the development and operational life of the system. (3) The process of controlling modifications to the system's hardware, firmware, software, and documentation that provides sufficient assurance that the system is protected against the introduction of improper modifications prior to, during, and after system implementation. (Compare configuration management.)

**configuration management:** The management of security features and assurances through control of changes made to a system's hardware, software, firmware, documentation, test, test fixtures, and test

documentation throughout the development and operational life of the system. (Compare configuration control.)

**confinement:** The prevention of the leaking of sensitive data from a program.

**confinement channel:** Synonymous with covert channel.

**confinement property:** Synonymous with \*-property (star property).

**connection:** A liaison, in the sense of a network interrelationship, between two hosts for a period of time. The liaison is established (by an initiating host) for the purpose of information transfer (with the associated host). The period of time is the time required to carry out the intent of the liaison (for example, transfer of a file, a chatter session, or delivery of mail). In many cases, a connection (in the sense of this glossary) will coincide with a host-host connection (in a special technical sense) that is established via TCP (Transmission Control Protocol) or an equivalent protocol. However, a connection (liaison) can also exist when only a protocol such as IP (Internet Protocol) is in use. (IP has no concept of a connection that persists for a period of time.) Hence, the notion of connection can be independent of the particular protocols in use during a liaison of two hosts.

**construction:** The process of creating a target of evaluation.

**consumers:** Individuals or groups responsible for specifying requirements for IT (information technology) product security (for example, policy makers and regulatory officials, system architects, integrators, acquisition managers, product purchasers, and end users).

**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.

**content-dependent access control:** Access control in which access is determined by the value of the data to be accessed.

**context-dependent access control:** Access control in which access is determined by the specific circumstances under which the data is being accessed.

**contingency plan:** A plan for emergency response, backup operations, and postdisaster recovery maintained by an activity 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. Synonymous with disaster plan and emergency plan.

**control objective:** Required result of protecting information within an IT (information technology) product and its immediate environment.

**control zone:** The space, expressed in feet of radius, surrounding equipment processing sensitive information, that is under sufficient physical and technical control to preclude an unauthorized entry or compromise.

**controlled access:** See access control.

**controlled sharing:** The condition that exists when access control is applied to all users and components of a system.

**corporate security policy:** The set of laws, rules, and practices that regulate how assets including sensitive information are managed, protected, and distributed within a user organization.

**correctness:** (1) A property of a representation of a target of evaluation such that it accurately reflects the stated security target for that system or product. Correctness consists of determining if the description and implementation are consistent. There are levels of correctness that depend on the evidence requirements and the intensity of verification and analysis. (2) In security evaluation, the preservation of relevant properties between successive levels of representations. Examples of representations could be top-level functional specification, detailed design specification, and actual implementation. This is an aspect of assurance. (3) Correctness in the draft Federal Criteria equates to assurance in the Information Technology Security Evaluation Criteria. Development and evaluation assurance constitute correctness criteria. Effectiveness is addressed in vetting of protection profiles. (4) The extent to which a program satisfies its specifications.

**cost-risk analysis:** The assessment of the costs of providing data protection for a system versus the cost of losing or compromising the data.

**countermeasure:** Action, device, procedure, technique, or other measure that reduces the vulnerability of a system, such as an AIS (automated information system).

**covert channel:** (1) A communication channel that allows a process to transfer information in a manner that violates the system's security policy. A covert channel typically communicates by exploiting a mechanism

not intended to be used for communication. (See covert storage channel and covert timing channel.) (2) The use of a mechanism not intended for communication to transfer information in a way that violates security. (3) Unintended and/or unauthorized communications path that can be used to transfer information in a manner that violates an AIS (automated information system) security policy. (See overt channel and exploitable channel.)

**covert storage channel:** A covert channel that involves the direct or indirect writing of a storage location by one process and the direct or indirect reading of the storage location by another process. Covert storage channels typically involve a finite resource (for example, sectors on a disk) that is shared by two subjects at different security levels.

**covert timing channel:** (1) A covert channel by which a process signals information to another process by modulating its own use of system resources (for example, CPU time) in such a way that this manipulation affects the real response time observed by the second process. (2) A communications channel that allows two cooperating processes to transfer information in a manner that violates the system's security policy. Synonymous with confinement channel.

**criteria:** See DoD Trusted Computer System Evaluation Criteria. Examples of other criteria are the Information Technology Security Evaluation Criteria (Europe), Canadian Trusted Computer Product Evaluation Criteria, Federal Criteria for Information Technology Security: Draft (US), and the forthcoming Common Criteria for Information Technology Security (international).

**critical mechanism:** A mechanism within a target of evaluation whose failure would create a security weakness.

**cryptoalgorithm:** A well-defined procedure or sequence of rules or steps used to produce a key stream or ciphertext from plaintext and vice versa.

**cryptography:** (1) The principles, means, and methods for rendering information unintelligible, and for restoring encrypted information to intelligible form. (2) The transformation of ordinary text, or "plaintext," into coded form by encryption and the transformation of coded text into plaintext by decryption. Cryptography can be used to support digital signature, key management or exchange, and communications privacy.

**cryptosecurity:** The security or protection resulting from the proper use of technically sound cryptosystems.

## D

**data:** Information with a specific physical representation.

**data confidentiality:** The state that exists when data is held in confidence and is protected from unauthorized disclosure.

**Data Encryption Standard (DES):** (1) A cryptographic algorithm for the protection of unclassified data, published in US Federal Information Processing Standard (FIPS) 46. The DES, which was approved by the US National Institute of Standards and Technology (NIST), is intended for public and government use. (2) A NIST Federal Information Processing Standard and commonly used secret key cryptographic algorithm for encrypting and decrypting data and performing other functions. For example, DES can be used to check message integrity. DES specifies a key length of 56 bits.

**data flow control:** Synonymous with information flow control.

**data integrity:** (1) The property that data has not been altered or destroyed in an unauthorized manner. (2) The state that exists when computerized data is the same as that in the source documents and has not been exposed to accidental or malicious alteration or destruction.

**data security:** The protection of data from unauthorized (accidental or intentional) modification, destruction, or disclosure.

**database management system:** 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.

**DBMS:** Abbreviation for database management system.

**declassification of AIS storage media:** An administrative decision or procedure to remove or reduce the security classification of the subject media.

**decomposition:** Requirement in a protection profile that spans several components. Note: The decomposition of a specific requirement becomes necessary when that requirement must be assigned to multiple components of the generic product requirements during the interpretation process.

**dedicated security mode:** See modes of operation.



**default classification:** A temporary classification reflecting the highest classification being processed in a system. The default classification is included in the caution statement affixed to the object.

**degauss:** To reduce magnetic flux density to zero by applying a reverse magnetizing field.

**degausser:** An electrical device that can generate a magnetic field for the purpose of degaussing magnetic storage media.

**Degausser Products List (DPL):** A list of commercially produced degaussers that meet US National Security Agency (NSA) specifications. This list is included in NSA's "Information Systems Security Products and Services Catalogue," available through the US Government Printing Office.

**delivery:** The process whereby a copy of the target of evaluation is transferred from the developer to a customer.

**denial of service:** (1) The prevention of authorized access to system assets or services or the delaying of time-critical operations. (2) Any action or series of actions that prevents any part of a system from functioning in accordance with its intended purpose. This includes any action that causes unauthorized destruction, modification, or delay of service. (Synonymous with interdiction.)

**dependency:** Condition in which the correctness of one TCB (trusted computing base) subset is contingent (depends for its correctness) on the correctness of another TCB subset. Note: A TCB subset A depends for its correctness on TCB subset B if and only if the (engineering) arguments of the correct implementation of A with respect to its specification assume, wholly or in part, that the specification of B has been implemented correctly.

**descriptive top level specification (DTLS):** A top-level specification that is written in a natural language (for example, English), an informal design notation, or a combination of the two.

**designated approving authority (DAA):** (1) Official with the authority to formally assume responsibility for operating an IT (information technology) product, an AIS (automated information system), or network at an acceptable level of risk. (2) The official who has the authority to decide on accepting the security safeguards prescribed for an AIS or that official who may be responsible for issuing an accreditation statement that records the decision to accept those safeguards.

**detailed design:** A phase of the development process wherein the top-level definition and design of a target of evaluation are refined and expanded to a level of detail that can be used as a basis for implementation.

**developer:** The person or organization that manufactures a target of evaluation.

**developer security:** The physical, procedural, and personnel security controls imposed by a developer on its development environment.

**development assurance:** (1) Establishes specific requirements to document appropriate aspects of the development process, the development environment, and operational support of the product. Development assurance specifies the manner in which products should be developed and/or details the amount and kind of evidence to be produced and retained during development. (2) Sources of IT (information technology) product assurance ranging from how a product was designed and implemented to how it is tested, operated, and maintained.

**development assurance component:** Fundamental building block, specifying how an IT (information technology) product is developed, from which development assurance requirements are assembled.

**development assurance package:** Grouping of development assurance components assembled to ease specification and common understanding of how an IT (information technology) product is developed.

**development assurance requirements:** Requirements in a protection profile that address how each conforming IT (information technology) product is developed, including the production of appropriate supporting developmental process evidence and how that product will be maintained.

**development environment:** The organizational measures, procedures, and standards used while constructing a target of evaluation.

**development process:** The set of phases and tasks whereby a target of evaluation is constructed, translating requirements into actual hardware and software.

**dial back:** Synonymous with call back.

**dial-up:** The service whereby a computer terminal can use the telephone to initiate and effect communication with a computer.

**digital signature:** A cryptographic method, provided by public key cryptography, used by a message's recipient and any third party to verify the identity of the message's sender. It can also be used to verify the authenticity of the message. A sender creates a digital signature on a message by transforming the message with his or her private key. A recipient, using the sender's public key, verifies the digital signature by applying a corresponding transformation to the message and the signature.

**Digital Signature Standard (DSS):** A US Federal Information Processing Standard proposed by NIST (National Institute of Standards and Technology) to support digital signature.

**digital telephony:** Telephone systems that use digital communications technology.

**disaster plan:** Synonymous with contingency plan.

**discretionary access control (DAC):** (1) A means of restricting access to objects based on the identity of subjects and/or groups to which they belong. The controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject (unless restrained by mandatory access control). (2) Methods of restricting access to objects or other resources based primarily on the instructions of arbitrary unprivileged users. Note: DAC is often used to enforce need-to-know.

**documentation:** The written (or otherwise recorded) information about a target of evaluation required for an evaluation. This information may, but need not, be contained within a single document produced for the specified purpose.

**DoD Trusted Computer System Evaluation Criteria (TCSEC):** A document published by the US 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."

**domain:** The unique context (for example, access control parameters) in which a program is operating — in effect, the set of objects that a subject has the ability to access. Note: A subject's domain determines which access control attributes an object must have for a subject operating in

that domain to have a designated form of access. (See process and subject.)

**dominate:** Security level S1 is said to dominate security level S2 if the hierarchical classification of S1 is greater than or equal to that of S2 and the nonhierarchical categories of S1 include all those of S2 as a subset.

**dominated by (the relation):** (1) A security level A is dominated by security level B if the clearance/classification in A is less than or equal to the clearance/classification in B and the set of access approvals (for example, compartment designators) in A is contained in (the set relation) the set of access approvals in B (that is, each access approval appearing in A also appears in B). Depending on the policy enforced (for example, non-disclosure or integrity), the definition of “less than or equal to” and “contained in” may vary. For example, the level of an object of high integrity (that is, an object which should be modifiable only by very trustworthy individuals) may be defined to be “less than” the level of an object of low integrity (that is, an object which is modifiable by everyone). (2) Security level A is dominated by security level B if (a) the clearance/classification in A is less than or equal to the clearance/classification in B, and (b) the set of access approvals (for example, compartment designators) in A is contained in the set of access approvals in B (that is, each access approval appearing in A also appears in B). This dominance relation is a special case of a partial order.

**dominates (the relation):** “Security level B dominates security level A” is synonymous with “security level A is dominated by security level B.” (See dominated by.)

## E

**ease of use:** An aspect of the assessment of the effectiveness of a target of evaluation, namely, that it cannot be configured or used in a manner which is insecure but which an administrator or end user would reasonably believe to be secure. Note: This term can be used as a reference for each type of item to be evaluated or under evaluation.

**effectiveness:** (1) A property of a target of evaluation representing how well it provides security in the context of its actual or proposed operational use. (2) In security evaluations, an aspect of assurance assessing how well the applied security functions and mechanisms working together will actually satisfy the security requirements. (3) Effectiveness is established by evaluation (vetting) of a protection profile (or security target, if there is no protection profile) description of anticipated threats,

intended method of use, and residual risk. Effectiveness includes establishing suitability for use in the specified environment.

**emanations:** See compromising emanations.

**embedded system:** A system that performs or controls a function, either in whole or in part, as an integral element of a larger system or subsystem.

**emergency plan:** Synonymous with contingency plan.

**emission security:** The protection resulting from all measures taken to deny unauthorized persons information of value that might be derived from interception and from an analysis of compromising emanations from systems.

**encryption:** The process of making information indecipherable to protect it from unauthorized viewing or use, especially during transmission or storage. Encryption is based on an algorithm and at least one key. Even if the algorithm is known, the information cannot be decrypted without the key(s).

**end-to-end encryption:** The protection of information passed in a telecommunications system by cryptographic means, from point of origin to point of destination.

**end user:** A person in contact with a target of evaluation who makes use only of its operational capability.

**Endorsed Tools List (ETL):** The list of formal verification tools endorsed by the US NCSC (National Computer Security Center) for the development of systems with high levels of trust.

**enhanced hierarchical development methodology:** 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 type checker, a theorem prover, and a multilevel security checker. Note: This methodology is not based on the hierarchical development methodology.

**entrapment:** The deliberate planting of apparent flaws in a system for the purpose of detecting attempted penetrations.

**environment:** (1) All entities — users, procedures, conditions, objects, AISs (automated information systems), and other IT (information tech-

nology) products — that interact with (affect the development, operation, and maintenance of) an IT product. (2) The aggregate of external procedures, conditions, and objects that affect the development, operation, and maintenance of a system.

**erasure:** A process by which a signal recorded on magnetic media is removed. Erasure is accomplished in two ways: (1) by alternating-current erasure, by which the information is destroyed by applying an alternating high and low magnetic field to the media; or (2) by direct-current erasure, by which the media are saturated by applying a unidirectional magnetic field.

**Evaluated Products List (EPL):** A list of equipment, hardware, software, and firmware that have been evaluated against, and found to be technically compliant, at a particular level of trust, with the DoD (US Department of Defense) TCSEC (Trusted Computer System Security Evaluation Criteria) by the NCSC (National Computer Security Center). The EPL is included in NSA's "Information Systems Security Products and Services Catalogue," which is available through the Government Printing Office.

**evaluation:** (1) Technical assessment of a component's, product's, subsystem's, or system's security properties that establishes whether the component, product, subsystem, or system meets a specific set of requirements, for example, defined evaluation criteria. Note: Evaluation is a term that causes much confusion in the security community, because it is used in many different ways. It is sometimes used in the general English sense (judgment or determination of worth or quality). Based on common usage of the term in the security community, one can distinguish between two types of evaluation: (a) evaluations that exclude the environment, and (b) evaluations that include the environment. This second type of evaluation, an assessment of a system's security properties with respect to a specific operational mission, is termed certification. Evaluations that exclude the environment are assessments of the security properties against a defined criterion. (2) The process — given a security policy, a consistent description of required security functions, and a targeted assurance level — of achieving assurance. Evaluation also includes the checking for security vulnerabilities (in relation to the security policy). (3) The assessment of an IT (information technology) system or product against defined evaluation criteria.

**evaluation assurance:** (1) Source of IT (information technology) product assurance based on the kind and intensity of the evaluation analysis performed on the product. (2) Specifies the nature and intensity of evaluation activities to be performed on a TOE (target of evaluation), based on the expected threat and the intended environments.

**evaluation assurance component:** Fundamental building block, specifying the type and the rigor of required evaluation activities, from which evaluation assurance requirements are assembled.

**evaluation assurance package:** Grouping of evaluation assurance components assembled to ease specification and common understanding of the type and the rigor of required evaluation activities.

**evaluation assurance requirements:** Requirements in a protection profile which address both the type and the rigor of activities that must occur during product evaluation.

**evaluation body or entity:** See certification body.

**evaluation criteria:** A set of requirements defining the conditions under which an evaluation is performed. These requirements can also be used in specification and development of systems and products.

**evaluator:** (1) The independent person or organization that performs an evaluation. (2) Individual or group responsible for the independent assessment of IT (information technology) product security (for example, product evaluators, system security officers, system certifiers, and system accreditors).

**evaluator actions:** A component of the evaluation criteria for a particular phase or aspect of evaluation, identifying what the evaluator must do to check the information supplied by the sponsor of the evaluator, and the additional activities he must perform.

**executive state:** (1) One of several states in which a system may operate and the only one in which certain privileged instructions may be executed. Such instructions cannot be executed when the system is operating in other (for example, user) states. Synonymous with supervisor state. (2) A privileged state that can be used by supervisory software for multitasking operations. Reliable multitasking requires protection, such as segment-level protection. For example, segment-level protection can have the following protection checks: (a) type check, (b) limit check, (c) restriction of addressable domain, (d) restriction of procedure entry points, and (e) restriction of instruction set.

**explain:** Give required information and show that it satisfies all relevant requirements.

**exploitable channel:** (1) Any channel that is usable or detectable by subjects external to the trusted computing base. (2) A covert channel that is

usable or detectable by subjects external to the AIS's (automated information system's) trusted computing base and can be used to violate the AIS's technical security policy. (See covert channel.) (3) Any information channel that is usable or detectable by subjects external to the trusted computing base whose purpose is to violate the security policy of the system. (See covert channel.)

**external security controls:** Measures that include physical, personnel, procedural, and administrative security requirements and a separate certification and accreditation process which govern physical access to an IT (information technology) product. Note: These measures constitute assumptions and boundary conditions that are part of the environment described in a protection profile.

## **F**

**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.

**fail soft:** Pertaining to the selective termination of affected nonessential processing when a hardware or software failure is detected in a system.

**failure access:** An unauthorized and usually inadvertent access to data resulting from a hardware or software failure in the system.

**failure control:** The methodology used to detect failures and provide fail-safe or fail-soft recovery from hardware and software failures in a system.

**fault:** A condition that causes a device or system component to fail to perform in a required manner.

**Federal Criteria for Information Technology Security (FC) (draft):** US draft security criteria for trusted systems.

**fetch protection:** (1) A system-provided restriction to prevent a program from accessing data in another user's segment of storage. (2) The aggregate of all processes and procedures in a system designed to inhibit unauthorized access, contamination, or elimination of a file.

**file security:** The means by which access to computer files is limited to authorized users only.

**flaw:** An error of commission, omission, or oversight in a system that allows protection mechanisms to be bypassed.



**flaw hypothesis methodology:** A system analysis and penetration technique where specifications and documentation for the system are analyzed and then flaws in the system are hypothesized. The list of hypothesized flaws is then prioritized on the basis of the estimated probability that a flaw actually 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 direct the actual testing of and/or penetration attack against the system.

**flow control:** See information flow control.

**formal access approval:** Documented approval by a data owner to allow access to a particular category of information.

**formal development methodology:** A collection of languages and tools that enforces a rigorous method of verification. This methodology uses the Ina Jo specification language for successive stages of system development, including identification and modeling of requirements, high-level design, and program design.

**formal model of security policy:** An underlying model of security policy expressed in a formal style, that is, an abstract statement of the important principles of security that a TOE (target of evaluation) will enforce.

**formal proof:** A complete and convincing mathematical argument, presenting the full logical justification for each proof step, for the truth of a theorem or set of theorems. The formal verification process uses formal proofs to show the truth of certain properties of formal specification and to show that computer programs satisfy their specifications. Automated tools may (but need not) be used to formulate and/or check the proof.

**formal security policy model:** (1) A mathematically precise statement of a security policy. To be adequately precise, such a model must represent the initial state of a system, the way in which the system progresses from one state to another, and a definition of a “secure” state of the system. To be acceptable as a basis for a TCB (trusted computing base), the model must be supported by a formal proof that if the initial state of the system satisfies the definition of a “secure” state and if all assumptions required by the model hold, then all future states of the system will be secure. Some formal modeling techniques include state-transition models, denotational semantics models, and algebraic specification models. (See Bell-LaPadula model and security policy model.) (2) Mathematically precise statement consisting of (a) a formal technical security policy (given by constraints on a product’s external interface and/or constraints on the handling of controlled entities internal to the product), (b) rules of opera-

tion that show how the definition of security is to be enforced, and (c) a formal proof showing that the rules of operation guarantee satisfaction of the definition of security.

**formal specification:** Statement about a product made using the restricted syntax and grammar of a formal reasoning system and a set of terms that have been precisely and uniquely defined or specified. Note: The formal statement should be augmented by an informal explanation of the conventions used and the ideas being expressed. A well-formed syntax and semantics with complete specification of all constructs used must be referenced.

**formal top level specification (FTLS):** A 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.

**formal verification:** The process of using formal proofs to demonstrate the consistency (design verification) between a formal specification of a system and a formal security policy model or (implementation verification) between the formal specification and its program implementation.

**front-end security filter:** (1) A process that is invoked to process data according to a specified security policy prior to releasing the data outside the processing environment or upon receiving data from an external source. (2) A process implemented in hardware or software that is logically separated from the remainder of the system to protect the system's integrity.

**functional component:** Fundamental building block, specifying what an IT (information technology) product must be capable of doing, from which functional protection requirements are assembled.

**functional package:** Grouping of functional components assembled to ease specification and common understanding of what an IT (information technology) product is capable of doing.

**functional protection requirements:** Requirements in a protection profile that address what conforming IT (information technology) products must be capable of doing.

**functional testing:** The portion of security testing in which the advertised features of a system are tested, under operational conditions, for correct operation.

**functional unit:** A functionally distinct part of a basic component.

**functionality:** (1) Set of functional protection requirements to be implemented in IT (information technology) products. (2) The totality of functional properties of a TOE (target of evaluation) that contributes to security.

**functionality class:** A defined set of security functions in a system or product, designed to meet a security policy.

## G

**general-purpose system:** A computer system that is designed to aid in solving a wide variety of problems.

**generic threat:** Class of threats with common characteristics pertaining to vulnerabilities, agents, event sequences, and resulting misfortunes.

**global requirements:** Those which require analysis of the entire system and for which separate analysis of the individual TCB (trusted computing base) subsets does not suffice.

**granularity:** (1) Relative fineness or coarseness to which an access control mechanism or other IT (information technology) product aspect can be adjusted. (2) An expression of the relative size of a data object. Note: Protection at the file level is considered coarse granularity, whereas protection at the field level is considered to be finer granularity. The phrase “the granularity of a single user” means the access control mechanism can be adjusted to include or exclude any single user.

**granularity of a requirement:** Determination of whether a requirement applies to all the attributes of users, subjects, or objects, and all TCB (trusted computing base) functional components.

**group:** Named collection of user identifiers.

**guard:** A processor that provides a filter between two disparate systems operating at different security levels or between a user terminal and a database to filter out data that the user is not authorized to access.

**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.

## H

**handshaking procedure:** A dialogue between two entities (for example, a user and a computer, a computer and another computer, or a program and another program) for the purpose of identifying and authenticating the entities to one another.

**hierarchical decomposition:** The ordered, structured reduction of a system or a component to primitives.

**hierarchical development methodology:** A methodology for specifying and verifying the design programs 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.

**host:** Any computer-based system connected to the network and containing the necessary protocol interpreter software to initiate network access and carry out information exchange across the communications network. This definition encompasses typical “mainframe” hosts, generic terminal support machines (for example, ARPAnet TAC, DoDIIS NTC), and workstations connected directly to the communications subnetwork and executing the intercomputer networking protocols. A terminal is not a host because it does not contain the protocol software needed to perform information exchange; a workstation (by definition) is a host because it does have such capability.

**host to front-end protocol:** A set of conventions governing the format and control of data that are passed from a host to a front-end machine.

## I

**identification:** Process that enables recognition of an entity by an IT (information technology) product/system that may be by the use of unique machine-readable user names.

**impersonating:** Synonymous with spoofing.

**implementation:** A phase of the development process wherein the detailed specification of a target of evaluation is translated into actual hardware and software.

**incomplete parameter checking:** A system design flaw that results when all parameters have not been fully anticipated for accuracy and consistency, thus making the system vulnerable to penetration.

**individual accountability:** The ability to associate positively the identity of a user with the time, method, and degree of access to a system.

**informal specification:** Statement about (the properties of) a product made using the grammar, syntax, and common definitions of a natural language (for example, English). Note: While no notational restrictions apply, the informal specification is also required to provide defined meanings for terms which are used in a context other than that accepted by normal usage.

**information flow control:** A procedure to ensure that information transfers within a system are not made from a higher security level object to an object of a lower security level. (See covert channel, simple security property, and \*-property (star property). Synonymous with data flow control and flow control.)

**information processing standard:** A set of detailed technical guidelines used to establish uniformity to support specific functions and/or interoperability in hardware, software, or telecommunications development, testing, and/or operation.

**information protection policy:** Set of laws, rules, and practices that regulate how an IT (information technology) product will, within specified limits, counter threats expected in the product's assumed operational environment.

**information system security officer (ISSO):** The person responsible to the DAA (designated approving authority) for ensuring that security is provided for and implemented throughout the life cycle of an AIS (automated information system) from the beginning of the concept development plan through its design, development, operation, maintenance, and secure disposal.

**Information Systems Security Products and Services Catalogue:** A catalogue issued quarterly by the National Security Agency that incorporates the DPL (Degausser Products List), EPL (Evaluated Products List), ETL (Endorsed Tools List), PPL (Preferred Products List), and other security product and service lists. This catalogue is available through the US Government Printing Office, Washington, DC 20402, (202) 783-3238.

**Information Technology Security Evaluation Criteria (ITSEC):** European security evaluation criteria for targets of evaluation (TOE).

**information technology (IT) system:** An international term for an information system, which consists of one or more automated information systems (AISs) or computer systems and communications systems.

**Integrated Services Digital Network:** An emerging communications system enabling the simultaneous transmission of data, facsimile, video, and voice over a single communications link.

**integrity:** (1) Correctness and appropriateness of the content and/or source of a piece of information. (See data integrity and system integrity.) (2) The prevention of the unauthorized modification of information. (3) Sound, unimpaired, or perfect condition.

**integrity policy:** A security policy to prevent unauthorized users from modifying — that is, writing — sensitive information. (See security policy.)

**interdiction:** See denial of service.

**internal security controls:** (1) Hardware, firmware, and software features within a system that restrict access to resources (hardware, software, and data) to authorized subjects only (persons, programs, or devices). (2) Mechanisms implemented in the hardware, firmware, and software of an IT (information technology) product which provide protection for the IT product.

**internal subject:** A subject that is not acting as a direct surrogate for a user. A process that is not associated with any user but performs system-wide functions such as packet switching, line printer spooling, and so on. (Also known as a daemon or a service machine.)

**interoperability:** The ability of computers to act upon information received from one another.

**isolation:** The containment of subjects and objects in a system in such a way that they are separated from one another, as well as from the protection controls of the operating system.

**IT (information technology) security:** The state of security in an IT system.

**IT (information technology) security certification:** The issue, by an independent body, of a formal statement or certificate confirming the results of an evaluation of a TOE (target of evaluation) and the fact that the

evaluation criteria used were correctly applied. Note: This term could also be called “TOE certification” to make its application clearer.

**IT (information technology) system:** A specific IT installation, with a particular purpose and operational environment.

## K

**key:** A long string of seemingly random bits used with cryptographic algorithms to create or verify digital signatures and encrypt or decrypt messages and conversations. The keys must be known or guessed to forge a digital signature or decrypt an encrypted message.

**key-escrow system:** An electronic means of reconstructing a secret key (for secret key encryption) or a private key (for public key encryption). The reconstructed key can then be used in a process to decrypt a communication.

**key management/exchange:** A method of electronically transmitting, in a secure fashion, a secret key for use with a secret key cryptographic system. Key management can be used to support communications privacy. This method can be accomplished most securely with public key cryptographic systems, which do not require the sharing of secret keys with third parties. Instead, a secret key is encrypted with a recipient’s public key, and the recipient decrypts the result with his or her private key to receive the secret key. A variation of key management that is based on key exchange does not require encrypting the secret key.

## L

**label:** See sensitivity label.

**lattice:** A partially ordered set for which every pair of elements has a greatest lower bound and a least upper bound.

**least privilege:** A principle that requires that each subject be granted the most restrictive set of privileges needed for the performance of authorized tasks. For certain applications, the most restrictive set of privileges could pertain to the lowest clearance. The application of this principle limits the damage that can result from accident, error, or unauthorized use of an AIS (automated information system).

**limited access:** Synonymous with access control.

**list-oriented:** A computer protection system in which each protected object has a list of all subjects authorized to access it. (Compare ticket-oriented.)

**local requirements:** Those for which separate analysis of the individual TCB (trusted computing base) subsets suffices to determine compliance for the composite TCB. (See the trusted database interpretation of the Trusted Computer System Evaluation Criteria for further information.)

**lock-and-key protection system:** A protection system that involves matching a key or password with a specific access requirement.

**logic bomb:** A resident computer program that triggers the perpetration of an unauthorized act when particular states of the system are realized.

**loophole:** An error of omission or oversight in software or hardware that permits circumvention of the system security policy.

## M

**magnetic remanence:** A measure of the magnetic flux density remaining after removal of the applied magnetic force. Refers to any data remaining on magnetic storage media after removal of the power.

**maintenance hook:** Special instructions in software to allow easy maintenance and additional feature development. These are not clearly defined during access for design specification. Hooks frequently allow entry into the code at unusual points or without the usual checks, so they are a serious security risk if they are not removed prior to live implementation. Maintenance hooks are special types of trap doors.

**malicious logic:** Hardware, software, or firmware that is intentionally included in a system for an unauthorized purpose — for example, a Trojan horse.

**mandatory access control:** A 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 (that is, clearance) of subjects to access information of such sensitivity. (See nondiscretionary access control. Compare discretionary access control.)

**masquerading:** Synonymous with spoofing.

**mass-market software:** Software that is (1) generally available to the public by sale, without restriction, from stock at retail selling points through



over-the-counter, telephone, and mail transactions and (2) designed for user installation without substantial supplier support.

**mechanism:** Operating system entry point or separate operating system support program that performs a specific action or related group of actions.

**metadata:** (1) Data referring to other data; data (such as data structures, indices, and pointers) 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 (for example, relations, domains, entities, or relationships) of a database.

**mimicking:** Synonymous with spoofing.

**modes of operation:** A description of the conditions under which an AIS (automated information system) functions, based on the sensitivity of data processed and the clearance levels and authorizations of the users. Four modes of operation are authorized:

(1a) An AIS is operating in the *dedicated mode* when the 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 specific period of time. (1b) An AIS is operating in the *dedicated mode* when each user with direct or indirect individual access to the AIS, its peripherals, its remote terminals, or its remote hosts has all of the following: (a) a valid personnel clearance for all information on the system, (b) formal access approval for, and signed nondisclosure agreements for, all the information stored and/or processed (including all compartments, subcompartments, and/or special access programs), and (c) a valid need-to-know for all information contained within the system.

(2a) An AIS is operating in the *system-high mode* when each user with direct or indirect access to the AIS, its peripherals, remote terminals, or remote hosts has all of the following: (a) a valid personnel clearance for all information on the AIS, (b) formal access approval for, and signed nondisclosure agreements for, all the information stored and/or processed (including all compartments, subcompartments, and/or special access programs), and (c) a valid need-to-know for some of the information contained within the AIS. (2b) An AIS is operating in the *system-high mode* when the system hardware and software are trusted only to provide discretionary protection between users. In this mode, the entire system, to include all components electrically and/or physically connected, must operate with security measures commensurate with the highest classification and sensitivity of the information being processed and/or stored.

All system users in this environment must possess clearances and authorization for all information contained in the system. All system output must be clearly marked with the highest classification and all system caveats until the information has been reviewed manually by an authorized individual to ensure appropriate classifications and that caveats have been affixed.

(3) An AIS is operating in the *compartmented mode* when each user with direct or indirect access to the AIS, its peripherals, remote terminals, or remote hosts has all of the following: (a) a valid personnel clearance for the most restricted information processed in the AIS, (b) formal access approval for, and signed nondisclosure agreements for, that information to which he or she is to have access, and (c) a valid need-to-know for that information to which he or she is to have access.

(4) An AIS is operating in the *multilevel mode* when all the following statements are satisfied concerning users with direct or indirect access to the AIS, its peripherals, remote terminals, or remote hosts: (a) some do not have a valid personnel clearance for all the information processed in the AIS, (b) all have the proper clearance and have the appropriate formal access approval for that information to which they are to have access, and (c) all have a valid need-to-know for that information to which they are to have access.

**monolithic TCB (trusted computing base):** A TCB that consists of a single TCB subset.

**multilevel device:** A device that is used in a manner that permits it to simultaneously process data of two or more security levels without risk of compromise. To accomplish this, sensitivity labels are normally stored on the same physical medium and in the same form (that is, machine-readable or human-readable) as the data being processed.

**multilevel mode:** See modes of operation.

**multilevel secure:** A class of system containing information with different sensitivities that simultaneously permits access by users with different security clearances and needs-to-know, but prevents users from obtaining access to information for which they lack authorization.

**multilevel security mode:** See modes of operation.

**multiple access rights terminal:** A terminal that may be used by more than one class of users — for example, users with different access rights to data.

**multiuser mode of operation:** A mode of operation designed for systems that process sensitive unclassified information in which users may not have a need-to-know for all information processed in the system. This mode is also for microcomputers processing sensitive unclassified information that cannot meet the requirements of the stand-alone mode of operation.

**mutually suspicious:** The state that exists between interacting processes (subsystems or programs) in which neither process can expect the other process to function securely with respect to some property.

## N

**National Computer Security Assessment Program:** A program designed to evaluate the interrelationship of empirical data of computer security infractions and critical systems profiles, while comprehensively incorporating information from the CSTVRP (Computer Security Technical Vulnerability Reporting Program). The assessment will build threat and vulnerability scenarios that are based on a collection of facts from relevant reported cases. Such scenarios are a powerful, dramatic, and concise form of representing the value of loss experience analysis.

**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 US Department of Defense.

**National Security Decision Directive 145 (NSDD 145):** Signed by US President Reagan on September 17, 1984, this directive is entitled “National Policy on Telecommunications and Automated Information Systems Security.” It provides initial objectives, policies, and an organizational structure to guide the conduct of national activities toward safeguarding systems that process, store, or communicate sensitive information; establishes a mechanism for policy development; and assigns implementation responsibilities. In 1990, National Security Directive 42 replaced NSDD 145, except for ongoing telecommunications protection activities mandated by NSDD 145 and Presidential Directive 24.

**National Telecommunications and Information Systems Security Advisory Memoranda/Instructions (NTISSAM, NTISSI):** Under NSDD (National Security Decision Directive) 145, NTISS Advisory Memoranda and Instructions provided advice, assistance, or information of general interest on telecommunications and systems security to all applicable US federal departments and agencies. NTISSAMs/NTISSIs were promulgated by the

National Manager for Telecommunications and Automated Information Systems Security. (See National Security Decision Directive 145.)

**National Telecommunications and Information System Security Directives (NTISSD):** Under NSDD 145, NTISS Directives established national-level decisions relating to NTISS policies, plans, programs, systems, or organizational delegations of authority. NTISSDs were promulgated by the Executive Agent of the US Government for Telecommunications and Information Systems Security, or by the chairman of the NTISSC when so delegated by the executive agent. NTISSDs were binding upon all federal departments and agencies. (See National Security Decision Directive 145.)

**need-to-know:** (1) Access to, or knowledge or possession of, specific information required to carry out official duties. (2) The necessity for access to, knowledge of, or possession of specific information required to carry out official duties.

**network architecture:** The set of layers and protocols (including formats and standards that different hardware and software must comply with to achieve stated objectives) which define a network.

**network component:** (1) A physical unit that does *not* provide a complete set of end-user services. A network component may support all or part of MDIA (mandatory access control, identification and authentication, and audit). This definition is used with the Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria Environments Guideline (TNIEG). (2) A network subsystem which is evaluatable for compliance with the trusted network interpretations, relative to that policy induced on the component by the overall network policy. Note: This definition is used with the Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria (TNI).

**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 (Transmission Control Protocol) connection. But also, when a host transmits an IP (Internet Protocol) datagram using only the services of its “connection-less” Internet Protocol interpreter, there is considered to be a connection between the source and the destination hosts for this transaction.

**network front end:** A device that implements the necessary network protocols, including security-related protocols, to allow a computer system to be attached to a network.

**network reference monitor:** An access control concept that refers to an abstract machine that mediates all access to objects within the network by subjects within the network.

**network security:** The protection of networks and their services from unauthorized modification, destruction, or disclosure — providing an assurance that the network performs its critical functions correctly and there are no harmful side effects. Includes providing for information accuracy.

**network security architecture:** A subset of network architecture specifically addressing security-relevant issues.

**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.

**network system:** A system that is implemented with a collection of interconnected network components. A network system is based on a coherent security architecture and design.

**network trusted computing base (NTCB):** The 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.)

**nondiscretionary access control:** Means of restricting access to objects based largely on administrative actions. (See mandatory access control.)

**normal operation:** Process of using a system.

**NSDD 145:** See National Security Decision Directive 145.

**NTCB (network trusted computing base) 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.

## O

**object:** (1) A passive entity that contains or receives information. Access to an object potentially 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. (See passive.) (2) A controlled entity that precisely gives or receives information in response to access attempts by another (active) entity.

**object reuse:** The reassignment and reuse of a storage medium (for example, page frame, disk sector, or magnetic tape) that once contained one or more objects. To be securely reused and assigned to a new subject, storage media must contain no residual data (magnetic remanence) from the object(s) previously contained in the media.

**open security environment:** An environment that includes those systems in which at least one of the following conditions holds true: (1) Application developers (including maintainers) do not have sufficient clearance or authorization to provide an acceptable presumption that they have not introduced malicious logic. (2) Configuration control does not provide sufficient assurance that applications are protected against the introduction of malicious logic prior to and during the operation of system applications.

**operating procedure:** A set of rules defining correct use of a target of evaluation.

**operation:** The process of using a target of evaluation.

**operational documentation:** The information produced by the developer of a target of evaluation to specify and explain how customers should use it.

**operational environment:** The organizational measures, procedures, and standards to be used while operating a target of evaluation.

**operations security (OPSEC):** An analytical process by which the US government and its supporting contractors can deny to potential adversaries information about capabilities and intentions by identifying, controlling, and protecting evidence of the planning and execution of sensitive activities and operations.

**Orange Book:** Alternate name for DoD (US Department of Defense) Trusted Computer Security Evaluation Criteria.

**organizational security policy:** Set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.

**OSI architecture:** The International Organization for Standardization (ISO) provides a framework for defining the communications process between systems. This framework includes a network architecture, consisting of seven layers. The architecture is referred to as the Open Systems Interconnection (OSI) Model or Reference Model. Services and the protocols to implement it for the different layers of the model are defined by international standards. From a systems viewpoint, the bottom three layers support the components of the network necessary to transmit a message, the next three layers generally pertain to the characteristics of the communicating end systems, and the top layer supports the end users. The seven layers are: (1) Physical Layer, (2) Link Layer, (3) Network Layer, (4) Transport Layer, (5) Session Layer, (6) Presentation Layer, and (7) Application Layer.

**output:** Information that has been exported by a TCB (trusted computing base).

**overt channel:** Communications path within a computer system or network that is designed for the authorized transfer of data. (See covert channel.)

**overwrite procedure:** A stimulation to change the state of a bit followed by a known pattern. (See magnetic remanence.)

**owner:** User-granted privileges with respect to security attributes and privileges affecting specific subjects and objects.

## P

**partial order:** A relation that is symmetric ( $a$  is related to  $a$ ), transitive (if  $a$  is related to  $b$  and  $b$  is related to  $c$ , then  $a$  is related to  $c$ ), and anti-symmetric (if  $a$  is related to  $b$  and  $b$  is related to  $a$ , then  $a$  and  $b$  are identical).

**partitioned security mode:** A mode of operation wherein all personnel have the clearance but not necessarily formal access approval and need-to-know for all information contained in the system. Not to be confused with compartmented security mode.

**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 (for example, monitoring and/or recording of data).

**password:** Protected/private character string used to authenticate an identity or to authorize access to data.

**penetration:** The successful act of bypassing the security mechanisms of a system.

**penetration study:** A study to determine the feasibility and methods for defeating controls of a system.

**penetration testing:** (1) Security testing in which evaluators attempt to circumvent the security features of an AIS (automated information system) based on their understanding of the system design and implementation. (2) Tests performed by an evaluator on the target of evaluation to confirm whether known vulnerabilities are actually exploitable in practice. (3) The portion of security testing in which the evaluators or penetrators attempt to circumvent the security features of a system. The evaluators or penetrators may be assumed to use all system design and implementation documentation, which may include listings of system source code, manuals, and circuit diagrams. The evaluators or penetrators work under no constraints other than those that would be applied to ordinary users or implementers of untrusted portions of the component.

**periods processing:** The processing of various levels of sensitive information at distinctly different times. 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.

**permissions:** A description of the type of authorized interactions a subject can have with an object. Examples include read, write, execute, add, modify, and delete.

**personal communications network:** Advanced cellular telephone communications and the interworking of both wired and wireless networks that will offer new communications services via very small, portable handsets. The network will rely on microcellular technology — many low-power, small-coverage cells — and a common channel-signaling technology, such as that used in the telephone system, to provide a wide variety of features in addition to the basic two-way calling service.



**personnel security:** The procedures established to ensure that all personnel who have access to sensitive information have the required authority as well as appropriate clearances.

**physical security:** The application of physical barriers and control procedures as preventive measures or countermeasures against threats to resources and sensitive information.

**piggyback:** Gaining unauthorized access to a system via another user's legitimate connection. (See *between-the-lines* entry.)

**plaintext:** See *cleartext*.

**Preferred Products List (PPL):** A list of commercially produced equipment that meets TEMPEST and other requirements prescribed by the US National Security Agency (NSA). This list is included in NSA's "Information Systems Security Products and Services Catalogue," issued quarterly and available through the Government Printing Office.

**primitive:** Orderly relation between TCB (trusted computing base) subsets based on dependency. Note: A TCB subset *B* is more primitive than a second TCB subset *A* (and *A* is less primitive than *B*) if *A* directly depends on *B* or 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.

**print suppression:** Eliminating the display of characters to preserve their secrecy — for example, not displaying the characters of a password as it is keyed at the input terminal.

**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. Note: The concept of privacy cannot be very precise, and its use should be avoided in specifications except as a means to require security, because privacy relates to "rights" that depend on legislation.

**private key:** The undisclosed key in a matched key pair — private key and public key — that each party safeguards for public key cryptography.

**privilege:** Special authorization that is granted to particular users to perform security-relevant operations.

**privileged instructions:** A set of instructions (for example, interrupt handling or special computer instructions) to control features (such as stor-

age protection features) that are generally executable only when the automated system is operating in the executive state.

**procedural security:** Synonymous with administrative security.

**process:** A program in execution. It is completely characterized by a single current execution point (represented by the machine state) and address space. (See domain and subject.)

**producers:** Providers of IT (information technology) product security (for example, product vendors, product developers, security analysts, and value-added resellers).

**product:** (1) A package of IT (information technology) software and/or hardware, providing functionality designed for use or incorporation within a multiplicity of systems. (2) A package of IT software and/or hardware designed to perform a specific function either stand alone or once incorporated into an IT system.

**product rationale:** (1) A description of the security capabilities of a product, giving the necessary information for a prospective purchaser to decide whether it will help to satisfy his system security objectives. (2) Overall justification — including anticipated threats, objectives for product functionality and assurance, technical security policy, and assumptions about the environments and uses of conforming products — for the protection profile and its resulting IT (information technology) product.

**production:** The process whereby copies of the target of evaluation are generated for distribution to customers.

**profile:** Detailed security description of the physical structure, equipment component, location, relationships, and general operating environment of an IT (information technology) product or AIS (automated information system). (See protection profile.)

**profile assurance:** Measure of confidence in the technical soundness of a protection profile.

**programming languages and compilers:** The tools used within the development environment in the construction of the software and/or firmware of a target of evaluation.

**proprietary information:** Information that is owned by a private enterprise and whose use and/or distribution is restricted by that enterprise. Note: Proprietary information may be related to the company's products, busi-

ness, or activities, including but not limited to financial information, data, or statements; trade secrets; product research and development information; existing and future product designs and performance specifications; marketing plans or techniques; schematics; client lists; computer programs; processes; and trade secrets or other company confidential information.

**protection-critical portions of the TCB (trusted computing base):** Those portions of the TCB whose normal function is to deal with the control of access between subjects and objects. Their correct operation is essential to the protection of the data on the system. (See subject, object, and trusted computing base.)

**protection philosophy:** (1) An informal description of the overall design of a system that delineates each of the protection mechanisms used. 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. (2) Informal description of the overall design of an IT (information technology) product that shows how each of the supported control objectives is dealt with.

**protection profile:** (1) An implementation-independent specification of the security requirements to be met by any of a set of possible products or systems. It is a high-level abstraction of the security target, and principally includes rationale, functional requirements, and assurance requirements. (2) Statement of security criteria shared by IT (information technology) 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.

**protection profile family:** Two or more protection profiles with similar functional requirements and rationale sections but with different assurance requirements.

**protection ring:** One of a hierarchy of privileged modes of a system that gives certain access rights to user programs and processes authorized to operate in a given mode.

**protocols:** A set of rules and formats, semantic and syntactic, that permits entities to exchange information.

**prove a correspondence:** Provide a formal correspondence, using a formal reasoning system (for example, 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.

**pseudoflaw:** An apparent loophole deliberately implanted in an operating system program as a trap for intruders.

**public key:** The key in a matched key pair — private key and public key — that may be published, for example, posted in a directory, for public key cryptography.

**public key cryptography:** Cryptography using two matched keys (or asymmetric cryptography) in which a single private key is not shared by a pair of users. Instead, users have their own key pairs. Each key pair consists of a matched private and public key. Public key cryptography can perform (1) digital signature, (2) secure transmission or exchange of secret keys, and/or (3) encryption and decryption. Examples of public key cryptography are DSS (Digital Signature Standard) and RSA (Rivest, Shamir, and Adleman).

**Public Law 100-235 (P.L. 100-235):** Also known as the Computer Security Act of 1987. This US law creates a means for establishing minimum acceptable security practices for improving the security and privacy of sensitive information in federal computer systems. The law assigns to the National Institute of Standards and Technology responsibility for developing standards and guidelines for federal computer systems processing unclassified data. The law also requires establishment of security plans by all operators of federal computer systems that contain sensitive information.

**purge:** The removal of sensitive data from an AIS (automated information system), AIS storage device, or peripheral device with storage capacity, at the end of a processing period. This action is performed in such a way that there is assurance proportional to the sensitivity of the data that the data may not be reconstructed. An AIS must be disconnected from any external network before a purge. After a purge, the medium can be declassified by observing the review procedures of the respective agency.

## R

**rating:** A measure for the assurance that may be held in a target of evaluation, consisting of a reference to its security target, an evaluation level established by assessment of the correctness of its implementation and consideration of its effectiveness in the context of actual or proposed operational use, and a confirmed rating of the minimum strength of its security mechanisms.

**RC2, RC4 (Rivest Cipher 2 and Rivest Cipher 4):** Two secret key encryption systems that are implemented in mass-market software. These systems are proprietary and are marketed by RSA Data Security, Inc. RC2 and RC4 can be used with various key lengths, such as 40 bits or 56 bits.

**read:** A fundamental operation that results only in the flow of information from an object to a subject.

**read access:** (1) Permission to read information. (2) A fundamental operation that results only in the flow of information from an object to a subject.

**read-only memory (ROM):** A storage area in which the contents can be read but not altered during normal computer processing.

**real time:** The actual time in which something, such as the communication of information, takes place.

**recovery procedures:** The actions necessary to restore a system's computational capability and data files after a system failure.

**reference monitor:** An access control/mediation concept that refers to an abstract machine that mediates all accesses to objects by subjects.

**reference monitor concept:** See reference monitor and security kernel.

**reference validation mechanism:** (1) Portion of a trusted computing base, the normal function of which is to mediate 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 the reference monitor. (2) An implementation of the reference monitor concept. A security kernel is a type of reference validation mechanism. (3) An implementation of the reference monitor concept that validates each reference to data or programs by any user (program) against a list of authorized types of reference for that user. It must be tamperproof, must always be invoked, and must be small enough to be subject to analysis and tests, the completeness of which can be assured.

**refinements:** Requirement in a protection profile taken to a lower level of abstraction than the component on which it is based. Note: The refinement of a component requirement is necessary when multiple environment-specific requirements must be assigned to a single component requirement.

**reliability:** (1) The extent to which a system can be expected to perform its intended function with required precision. (2) The probability of a given system performing its mission adequately for a specified period of time under the expected operating conditions.

**requirements:** (1) A phase of the development process wherein the security target of a target of evaluation is produced. (2) Phase of the development process wherein the top-level definition of the functionality of the system is produced.

**requirements for content and presentation:** A component of the evaluation criteria for a particular phase or aspect of evaluation identifying what each item of documentation identified as relevant to that phase or aspect of evaluation shall contain and how its information is to be presented.

**requirements for evidence:** A component of the evaluation criteria for a particular phase or aspect of evaluation defining the nature of the evidence to show that the criteria for that phase or aspect have been satisfied.

**requirements for procedures and standards:** A component of the evaluation criteria for a particular phase or aspect of evaluation identifying the nature and/or content of procedures or standard approaches that shall be adopted or utilized when the TOE (target of evaluation) is placed into live operation.

**residual risk:** Portion of risk that remains after security measures have been applied.

**residue:** Data left in storage after processing operations are complete, but before degaussing or rewriting has taken place.

**resource:** Anything used or consumed while performing a function. Note: The categories of resources include time, information, objects (information containers), or processors (the ability to use information). Specific examples include CPU (central processing unit) time, terminal connect time, amount of directly addressable memory, disk space, and number of I/O (input/output) requests per minute.

**resource encapsulation:** The process of ensuring that a resource is not directly accessible by a subject, but that it is protected so that the reference monitor can properly mediate accesses to it.

**restricted area:** Any area to which access is subject to special restrictions or controls for reasons of security or safeguarding of property or material.

**risk:** (1) The expected loss due to, or impact of, anticipated threats in light of system vulnerabilities and strength or determination of relevant threat agents. (2) The probability that a particular threat will exploit a particular vulnerability of the system.

**risk analysis:** The process of identifying security risks, determining their magnitude, and identifying areas needing safeguards. Risk analysis is a part of risk management. (Synonymous with risk assessment.)

**risk assessment:** Synonymous with risk analysis.

**risk index:** The disparity between the minimum clearance or authorization of system users and the maximum sensitivity (for example, classification and categories) of data processed by a system. (A complete explanation of this term is provided in CSC-STD-003-85 and CSC-STD-004-85 — US government publications.)

**risk management:** The total process of identifying, controlling, and eliminating or minimizing uncertain events that may affect system resources. It includes risk analysis, cost-benefit analysis, selection, implementation and test, security evaluation of safeguards, and overall security review.

**RSA:** A public key algorithm invented by Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman (RSA). RSA can be used to generate digital signatures, encrypt messages, and provide key management for DES (Data Encryption Standard), RC2 (Rivest Cipher 2), RC4 (Rivest Cipher 4), and other secret key algorithms. RSA performs the key management process, in part, by encrypting a secret key for an algorithm such as DES, RC2, or RC4 with the recipient's public key for secure transmission to the recipient. This secret key can then be used to support private communications.

## S

**safeguards:** See security safeguards.

**scavenging:** Searching through object residue to acquire unauthorized data.

**scope of a requirement:** Determination of whether a requirement applies to: all users, subjects, and objects of the TCB (trusted computing base); all the TCB commands and application programming interfaces; all TCB elements; all configurations; or only a defined subset of configurations.

**secrecy policy:** A security policy to prevent unauthorized users from reading sensitive information. (See security policy.)

**secret key:** The key that two parties share and keep secret for secret key cryptography. Given secret key algorithms of equal strength, the approximate difficulty of decrypting encrypted messages by brute force search can be measured by the number of possible keys. For example, a key length of 56 bits is over 65,000 times stronger or more resistant to attack than a key length of 40 bits.

**secret key cryptography:** Cryptography based on a single key (or symmetric cryptography). It uses the same secret key for encryption and decryption. Messages are encrypted using a secret key and a secret key cryptographic algorithm, such as Skipjack, DES (Data Encryption Standard), RC2 (Rivest Cipher 2), or RC4 (Rivest Cipher 4).

**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.

**secure state:** A condition in which no subject can access any object in an unauthorized manner.

**secure subsystem:** A subsystem that contains its own implementation of the reference monitor concept for those resources it controls. However, the secure subsystem must depend on other controls and the base operating system for the control of subjects and the more primitive system objects.

**security:** (1) The combination of confidentiality, integrity, and availability. (2) The quality or state of being protected from uncontrolled losses or effects. Note: Absolute security may in practice be impossible to reach; thus the security "quality" could be relative. Within state models of security systems, security is a specific "state" that is to be preserved under various operations.

**security architecture:** The subset of computer architecture dealing with the security of the computer or network system. (See computer architecture and network architecture.)

**security audit trail:** The set of records that collectively provide documentary evidence of processing used to aid in tracing from original transactions forward to related records and reports, and/or backward from records and reports to their component source transactions.

**security-compliant channel:** A channel is security compliant if the enforcement of the network policy depends only upon characteristics of the



channel either (1) included in the evaluation or (2) assumed as an installation constraint and clearly documented in the trusted facility manual.

**security-critical mechanisms:** Those security mechanisms whose correct operation is necessary to ensure that the security policy is enforced.

**security enforcing:** That which directly contributes to satisfying the security objectives of the target of evaluation.

**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 assurances 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.

**security fault analysis:** A security analysis, usually performed on hardware at gate level, to determine the security properties of a device when a hardware fault is encountered.

**security features:** The security-relevant functions, mechanisms, and characteristics of system hardware and software. Security features are a subset of system security safeguards.

**security filter:** A trusted subsystem that enforces a security policy on the data that pass through it.

**security flaw:** An error of commission or omission in a system that may allow protection mechanisms to be bypassed.

**security flow analysis:** A security analysis performed on a formal system specification that locates potential flows of information within the system.

**security kernel:** The hardware, firmware, and software elements of a trusted computing base (or network trusted computing base partition) that implement the reference monitor concept. It must mediate all accesses, be protected from modification, and be verifiable as correct.

**security label:** See sensitivity label.

**security level:** The combination of a hierarchical classification and a set of nonhierarchical categories that represents the sensitivity of information.

**security measures:** Elements of software, firmware, hardware, or procedures that are included in a system for the satisfaction of security specifications.

**security mechanism:** (1) That which implements a security function. (2) The logic or algorithm that implements a particular security-enforcing or security-relevant function in hardware and software.

**security objectives:** The contribution to security that a system or product is intended to achieve.

**security perimeter:** The boundary where security controls are in effect to protect assets.

**security policy:** (1) A set of rules and procedures regulating the use of information, including its processing, storage, distribution, and presentation. (See corporate security policy, system security policy, and technical security policy.) (2) The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.

**security policy model:** (1) A formal presentation of the security policy enforced by the system. It must identify the set of rules and practices that regulate how a system manages, protects, and distributes sensitive information. (See Bell-LaPadula model and formal security policy model.) (2) An informal presentation of a formal security policy model. Note: This is the original definition from the US Trusted Computer System Evaluation Criteria.

**security range:** The highest and lowest security levels that are permitted in or on a system, system component, subsystem, or network.

**security relevant:** That which is not security enforcing, but must function correctly for the target of evaluation to enforce security.

**security-relevant event:** Any event that attempts to change the security state of the system (for example, change access controls, change the security level of a user, change a user password). Also, any event that attempts to violate the security policy of the system (for example, too many attempts to log in, attempts to violate the mandatory access control limits of a device, attempts to downgrade a file, and so on).

**security requirements:** The types and levels of protection necessary for equipment, data, information, applications, and facilities to meet security policy.

**security requirements baseline:** A description of minimum requirements necessary for a system to maintain an acceptable level of security.

**security safeguards:** The protective measures and controls that are prescribed to meet the security requirements specified for a system. Those safeguards may include but are not necessarily limited to hardware and software security features, operating procedures, accountability procedures, access and distribution controls, management constraints, personnel security, and physical structures, areas, and devices. Also called safeguards.

**security specifications:** A detailed description of the safeguards required to protect a system.

**security target:** (1) 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 used. (2) Product-specific description, elaborating the more general requirements in a protection profile and including all evidence generated by the producers, of how a specific IT (information technology) product meets the security requirements of a given protection profile.

**security test and evaluation:** An examination and analysis of the security safeguards of a system as they have been applied in an operational environment to determine the security posture of the system.

**security testing:** A process used to determine that the security features of a system are implemented as designed and that they are adequate for a proposed application environment. This process includes hands-on functional testing, penetration testing, and verification. (See functional testing, penetration testing, and verification.)

**sensitive information:** (1) Information that, as determined by a competent authority, must be protected because its unauthorized disclosure, alteration, loss, or destruction will at least cause perceivable damage to someone or something. (2) Any information, the loss, misuse, modification of, or unauthorized access to, could affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, US Code, but that has not been specifically

authorized under criteria established by an executive order or an act of Congress to be kept classified in the interest of national defense or foreign policy.

**sensitivity label:** A piece of information that represents the security level of an object and that describes the sensitivity (for example, classification) of the data in the object. Sensitivity labels are used by the TCB (trusted computing base)/NTCB (network trusted computing base) as the basis for mandatory access control decisions.

**sensitivity level:** See security level.

**shall:** Indication that a requirement must be met unless a justification of why it cannot be met is given and accepted.

**should:** Indication of an objective requirement that requires less justification for nonconformance and should be more readily approved. Note: “Should” is often used when a specific requirement is not feasible in some situations or with common current technology.

**simple security condition:** See simple security property.

**simple security property:** A Bell-LaPadula security model rule allowing a subject read access to an object only if the security level of the subject dominates the security level of the object. Synonymous with simple security condition.

**single-level device:** A device that is used to process data of a single security level at any one time. Since the device need not be trusted to separate data of different security levels, sensitivity labels do not have to be stored with the data being processed.

**site certification:** The comprehensive assessment of the technical and nontechnical security functions of an IT (information technology) system in its operational environment to establish the extent to which the system meets a set of specified security requirements, performed to support operational system accreditation.

**Skipjack:** A classified 64-bit block encryption, or secret key encryption, algorithm. The algorithm uses 80-bit keys (compared with 56 for DES) and has 32 computational rounds or iterations (compared with 16 for DES). Skipjack supports all DES modes of operation. Skipjack provides high-speed encryption when implemented in a key-escrow chip.

**software development methodologies:** Methodologies for specifying and verifying design programs for system development. Each methodology is written for a specific computer language. (See enhanced hierarchical development methodology, formal development methodology, Gypsy verification environment, and hierarchical development methodology.)

**software security:** General-purpose (executive, utility, or software development tools) and applications programs or routines that protect data handled by a system.

**software system test and evaluation process:** A process that plans, develops, and documents the quantitative demonstration of the fulfillment of all baseline functional performance, operational, and interface requirements.

**sponsor:** The person or organization that requests an evaluation.

**spoofing:** An attempt to gain access to a system by posing as an authorized user. (Synonymous with impersonating, masquerading, and mimicking.)

**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 (for example, 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 (for example, a personal computer with nonremovable storage media such as a hard disk).

**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 (for example, a personal computer with removable storage media such as a floppy disk).

**star (\*) property:** See \*-property (at the beginning of the Glossary).

**state:** Give required information with no attempted or implied requirement, to justify the information presented.

**state delta verification system:** A system designed to give high confidence regarding microcode performance by using formulas that represent isolated states of a computation to check proofs concerning the course of that computation.

**state variable:** A variable that represents either the state of the system or the state of some system resource.

**storage object:** An object that supports both read and write accesses.

**strength of a requirement:** Definition of the conditions under which a functional component withstands a defined attack or tolerates failures.

**strength of mechanism:** A rating of the ability of a security mechanism to withstand a direct attack.

**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.

**Subcommittee on Automated Information Systems Security (SAISS):** NSDD (National Security Decision Directive) 145 authorized and directed the establishment, under the NTISSC (National Telecommunications and Information Systems Security Committee), of a permanent Subcommittee on Automated Information Systems Security (SAISS). The SAISS is composed of one voting member from each US federal organization represented on the NTISSC. In 1990, the NTISSC was replaced with the NSTISSC (National Security Telecommunications and Information Systems Security Committee) pursuant to NSD-42.

**Subcommittee on Telecommunications Security (STS):** NSDD (National Security Decision Directive) 145 authorized and directed the establishment, under the NTISSC (National Telecommunications and Information Systems Security Committee), of a permanent Subcommittee on Telecommunications Security (STS). The STS is composed of one voting member from each US federal organization represented on the NTISSC. In 1990, the NTISSC was replaced with the NSTISSC (National Security Telecommunications and Information Systems Security Committee) pursuant to NSD-42.

**subject:** Active entity in an IT (information technology) product or AIS (automated information system), generally in the form of a process or device, that causes information to flow among objects or changes the system state.

**subject security level:** A subject's security level is equal to the security level of the objects to which it has both read and write access. A subject's security level must always be dominated by the clearance of the user the subject is associated with.

**subset domain:** A set of system domains. For evaluation by parts, each candidate TCB (trusted computing base) subset must occupy a distinct

subset domain such that modify-access to a domain within a TCB subset's subset domain is permitted only to that TCB subset and (possibly) to more primitive TCB subsets.

**suitability of functionality:** An aspect of the assessment of the effectiveness of a target of evaluation, namely, the suitability of its security-enforcing functions and mechanisms to in fact counter the threats to the security of the target of evaluation identified in its security target.

**supervisor state:** Synonymous with executive state.

**system:** (1) A specific IT (information technology) installation, with a particular purpose and operational environment. (2) An assembly of computer and/or communications hardware, software, and firmware configured for the purpose of classifying, sorting, calculating, computing, summarizing, transmitting, receiving, storing, and retrieving data with the purpose of supporting users. (3) IT products assembled together — either directly or with additional computer hardware, software, and/or firmware — configured to perform a particular function within a particular operational environment.

**system development methodologies:** Methodologies developed through software engineering to manage the complexity of system development. Development methodologies include software engineering aids and high-level design analysis tools.

**system entry:** Mechanism by which an identified and authenticated user is provided access into the system.

**system high:** The highest security level supported by a system at a particular time or in a particular environment.

**system-high security mode:** See modes of operation.

**system integrity:** (1) The quality of a system fulfilling its operational purpose while (a) preventing unauthorized users from making modifications to resources or using resources, and (b) preventing authorized users from making improper modifications to resources or making improper use of resources. (2) The quality that a system has when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

**system low:** The lowest security level supported by a system at a particular time or in a particular environment.

**system security officer (SSO):** See information system security officer.

**system security policy:** The set of laws, rules, and practices that regulate how sensitive information and other resources are managed, protected, and distributed within a specific system.

**Systems Security Steering Group:** The senior US government body established by NSDD (National Security Decision Directive) 145 to provide top-level review and policy guidance for the telecommunications security and automated information systems security activities of the US government. This group is chaired by the Assistant to the President for National Security Affairs and consists of the Secretary of State, Secretary of Treasury, Secretary of Defense, Attorney General, Director of the Office of Management and Budget, and Director of Central Intelligence. In 1990, NSDD 145 was partially replaced by NSD-42.

## T

**tampering:** An unauthorized modification that alters the proper functioning of equipment or a system in a manner that degrades the security or functionality it provides.

**target of evaluation (TOE):** An IT (information technology) system, product, or component that is identified/subjected as requiring security evaluation.

**TCB (trusted computing base) 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.

**technical attack:** An attack that can be perpetrated by circumventing or nullifying hardware and software protection mechanisms, rather than by subverting system personnel or other users.

**technical policy:** (1) The set of rules regulating access of subjects to objects enforced by a TCB (trusted computing base) subset. (2) The set of rules regulating access of subjects to objects enforced by a computer system.



**technical security policy:** (1) Specific protection conditions and/or protection philosophy that expresses the boundaries and responsibilities of the IT (information technology) product in supporting the information protection policy control objectives and countering expected threats. (2) The set of laws, rules, and practices regulating the processing of sensitive information and the use of resources by the hardware and software of an IT system or product.

**technical vulnerability:** A hardware, firmware, communication, or software flaw that leaves a computer processing system open for potential exploitation, either externally or internally, thereby resulting in risk for the owner, user, or manager of the system.

**TEMPEST:** The study and control of spurious electronic signals emitted by electrical equipment, such as computer equipment.

**terminal identification:** The means used to uniquely identify a terminal to a system.

**threat:** (1) An action or event that might prejudice security. (2) Sequence of circumstances and events that allows a human or other agent to cause an information-related misfortune by exploiting a vulnerability in an IT (information technology) product. (3) Any circumstance or event with the potential to cause harm to a system in the form of destruction, disclosure, modification of data, or denial of service.

**threat agent:** A method used to exploit a vulnerability in a system, operation, or facility.

**threat analysis:** The examination of all actions and events that might adversely affect a system or operation.

**threat monitoring:** The analysis, assessment, and review of audit trails and other data collected for the purpose of searching out system events that may constitute violations or attempted violations of system security.

**ticket-oriented:** A computer protection system in which each subject maintains a list of unforgeable bit patterns, called tickets, one for each object the subject is authorized to access. (Compare list-oriented.)

**time-dependent password:** A password that is valid only at a certain time of day or during a specified interval of time.

**tool:** A product used in the construction and/or documentation of a target of evaluation.

**top-level specification (TLS):** A nonprocedural description of system behavior at the most abstract level — typically, a functional specification that omits all implementation details.

**trace a correspondence:** Explain a correspondence, using natural language prose, between levels of abstraction.

**tranquillity:** A security model rule stating that the security level of an object cannot change while the object is being processed by an AIS (automated information system).

**transaction:** Set of subject actions and their associated data storage accesses.

**transmission security:** Maintaining confidentiality of information in a telecommunications network.

**trap door (or trapdoor):** (1) Hidden software or hardware mechanism that can be triggered to permit protection mechanisms in an automated information system to be circumvented. Note: A trap door is usually activated in some innocent-appearing manner (for example, 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. (2) A secret entry point to a cryptographic algorithm through which the developer or another entity can bypass security controls and decrypt messages.

**Trojan horse:** A computer program with an apparently or actually useful function that contains additional (hidden) functions that surreptitiously exploit the legitimate authorizations of the invoking process to the detriment of security — for example, making a “blind copy” of a sensitive file for the creator of the Trojan horse.

**trusted channel:** A mechanism by which two NTCB (network trusted computing base) partitions can communicate directly. This mechanism can be activated by either of the NTCB partitions, cannot be imitated by untrusted software, and maintains the integrity of information that is sent over it. A trusted channel may be needed for the correct operation of other security mechanisms.

**trusted computer system:** A system that uses sufficient hardware and software assurance/integrity measures to allow its use for processing simultaneously a range of sensitive or classified information.

**trusted computing base (TCB):** The totality of protection mechanisms within a computer system, including hardware, firmware, and software, the combination of which is responsible for enforcing a security policy. A TCB consists of one or more components that enforce a unified security policy over a product or system. The ability of a TCB to correctly enforce a security policy depends solely on the mechanisms within the TCB and on the correct input by system administrative personnel of parameters (for example, a user's clearance) related to the security policy.

**trusted distribution:** A trusted method for distributing the TCB (trusted computing base) hardware, software, and firmware components, both originals and updates, that provides methods for protecting the TCB from modification during distribution and for detection of any changes to the TCB that may occur.

**trusted functionality:** That which is determined to be correct with respect to some criteria, for example, as established by a security policy. The functionality shall neither fall short of nor exceed the criteria.

**trusted identification forwarding:** An identification method used in networks whereby the sending host can verify that an authorized user on its system is attempting a connection to another host. The sending host transmits the required user authentication information to the receiving host. The receiving host can then verify that the user is validated for access to its system. This operation may be transparent to the user.

**trusted path:** A mechanism by which a person at a terminal can communicate directly with the trusted computing base. This mechanism can be activated only by the person or by the trusted computing base and cannot be imitated by untrusted software.

**trusted process:** A process whose incorrect or malicious execution is capable of violating system security policy.

**trusted software:** The software portion of a trusted computing base.

**trusted subject:** (1) A subject that is part of the TCB (trusted computing base). It has the ability to violate the security policy, but is trusted not to actually do so. For example, in the Bell-LaPadula model, a trusted subject is not constrained by the \*-property and thus has the ability to write sensitive information into an object whose level is not dominated by the (maximum) level of the subject, but it is trusted to only write information into objects with a label appropriate for the actual level of the information. (2) A subject that is permitted to have simultaneous view and alter-access to objects of more than one sensitivity level.

## U

**untrusted process:** A process that has not been evaluated or examined for adherence to the security policy. It may include incorrect or malicious code that attempts to circumvent the security mechanisms.

**usage security policy:** Assumptions regarding the expected environment and intended method of IT (information technology) product use.

**user:** (1) Any person who interacts directly with a computer system. (2) Any person who interacts directly with a network system. This includes both those persons who are authorized to interact with the system and those people who interact without authorization (for example, active or passive wire-tappers). Note that “users” do not include “operators,” “system programmers,” “technical control officers,” “system security officers,” and other system support personnel. They are distinct from users and are subject to the trusted facility manual and the system architecture requirements. Such individuals may change the system parameters of the network system, for example, by defining membership of a group. These individuals may also have the separate role of users. (3) Any person or process accessing an IT (information technology) product by direct connections (for example, 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.

**user documentation:** The information about a target of evaluation supplied by the developer for use by its end users.

**user identifier (user ID):** Unique symbol or character string that is used by an IT (information technology) system or product to uniquely identify a specific user.

**user profile:** Patterns of a user’s activity that can be used to detect changes in normal routines.

## V

**validation:** The process of assessing the usefulness of a system in relation to its intended use or purpose.

**verification:** (1) The process of ensuring correctness. (2) The process of comparing two levels of system specification for proper correspondence (for example, security policy model with top-level specification (TLS), TLS with source code, or source code with object code). This process may or may not be automated.

**view:** That portion of the database that satisfies the conditions specified in a query.

**view definition:** A stored query, sometimes loosely referred to as a “view.”

**virus:** (1) Malicious software, a form of Trojan horse, which reproduces itself in other executable code. (2) A self-propagating Trojan horse, composed of a mission component, a trigger component, and a self-propagating component. (3) Self-replicating malicious program segment that attaches itself to an application or other executable system component and leaves no external signs of its presence.

**vulnerability:** (1) A security weakness in a target of evaluation (for example, due to failures in analysis, design, implementation, or operation). (2) Weakness in an information system or components (for example, system security procedures, hardware design, or internal controls) that could be exploited to produce an information-related misfortune. (3) A weakness in system security procedures, system design, implementation, internal controls, and so on, that could be exploited to violate system security policy.

**vulnerability analysis:** The systematic examination of systems to determine the adequacy of security measures, identify security deficiencies, and provide data from which to predict the effectiveness of proposed security measures.

**vulnerability assessment:** (1) An aspect of the assessment of the effectiveness of a target of evaluation, namely, whether known vulnerabilities in that target of evaluation could in practice compromise its security as specified in the security target. (2) 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.

## W

**wiretapping:** The real-time collection of transmitted data, such as dialed digits, and the sending of that data in real time to a listening device.

**work factor:** An estimate of the effort or time needed by a potential penetrator with specified expertise and resources to overcome a protective measure.

**write:** A fundamental operation that results only in the flow of information from a subject to an object.

**write access:** Permission to write an object.