

Definitions

A

A1

Highest level of trust defined in the Orange Book (Department of Defense Trusted Computer System Evaluation Criteria, DoD 5200.28-STD).

Access

Opportunity to make use of an information system (IS) resource.

Access control

Limiting access to information system resources only to authorized users, programs, processes, or other systems.

Access control list (ACL)

Mechanism implementing discretionary and/or mandatory access control between subjects and objects.

Access control mechanism

Security safeguard designed to detect and deny unauthorized access and permit authorized access in an IS.

Access control officer (ACO)

Designated individual responsible for limiting Access to information systems resources.

Access level

Hierarchical portion of the security level used to identify the sensitivity of IS data and the clearance or authorization of users. Access level, in conjunction with the nonhierarchical categories, forms the sensitivity label of an object. See category.

Access list

(IS) Compilation of users, programs, or processes and the access levels and types to which each is authorized. (COMSEC) Roster of persons authorized admittance to a controlled area.

Access period

Segment of time, generally expressed in days or weeks, during which access rights prevail.

Access profile

Associates each user with a list of protected objects the user may access.

Access type

Privilege to perform action on an object. Read, write, execute, append, modify, delete, and create are examples of access types.

Accountability

(IS) Process of tracing IS activities to a responsible source.(COMSEC) Principle that an individual is entrusted to safeguard and control equipment, keying material, and information and is answerable to proper authority for the loss or misuse of that equipment or information.

Accreditation

Formal declaration by a Designated Approving Authority (DAA) that an IS is approved to operate in a particular security mode at an acceptable level of risk, based on the implementation of an approved set of technical, managerial, and procedural safeguards.

Accreditation package

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

Accrediting authority

Synonymous with Designated Approving Authority (DAA).

Add-on security

Incorporation of new hardware, software, or firmware safeguards in an operational IS.

Advisory

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

Alert

Notification that a specific attack has been directed at the IS of an organization.

Anti-jam

Measures ensuring that transmitted information can be received despite deliberate jamming attempts.

Anti-spoof

Measures preventing an opponent's participation in an IS.

Assurance

See information assurance.

Attack

Type of incident involving the intentional act of attempting to bypass one or more security controls (see Information Assurance) of an IS.

Audit trail

Chronological record of system activities to enable the reconstruction and examination of the sequence of events and/or changes in an event. Audit trail may apply to information in an IS, to message routing in a communications system, or to the transfer of COMSEC material.

Authenticate

To verify the identity of a user, user device, or other entity, or the integrity of data stored, transmitted, or otherwise exposed to unauthorized modification in an IS, or to establish the validity of a transmission.

Authentication

Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.

Authenticator

Means used to confirm the identity of a station, originator, or individual.

Authorization

Access privileges granted to a user, program, or process.

Authorized vendor

Manufacturer of INFOSEC equipment authorized to produce quantities in excess of contractual requirements for direct sale to eligible buyers. Eligible buyers are typically U.S. Government organizations or U.S. Government contractors.

Automated security monitoring

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

Availability

Timely, reliable access to data and information services for authorized users.

B

Back door

Hidden software or hardware mechanism used to circumvent security controls. Synonymous with trap door.

Backup

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

Banner

Display on an IS that sets parameters for system or data use.

Benign

Condition of cryptographic data that cannot be compromised by human access.

Benign environment

Nonhostile environment that may be protected from external hostile elements by physical, personnel, and procedural security countermeasures.

Biometrics

Automated methods of authenticating or verifying an individual based upon a physical or behavioral characteristic.

Bit error rate

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

BLACK

Designation applied to information systems, and to associated areas, circuits, components, and equipment, in which national security information is encrypted or is not processed.

Boundary

Software, hardware, or physical barrier that limits access to a system or part of a system.

Brevity list

List containing words and phrases used to shorten messages.

Browsing

Act of searching through IS storage to locate or acquire information, without necessarily knowing the existence or format of information being sought.

C

Call back

Procedure for identifying and authenticating a remote IS terminal, whereby the host system disconnects the terminal and reestablishes contact. Synonymous with dial back.

Capability

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

Cascading

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

Category

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

Certificate

Record holding security information about an IS user and vouches to the truth and accuracy of the information it contains.

Certificate management

Process whereby certificates (as defined above) are generated, stored, protected, transferred, loaded, used, and destroyed.

Certificate revocation list

List of invalid certificates (as defined above) that (CRL) have been revoked by the issuer.

Certification

Comprehensive evaluation of the technical and nontechnical security safeguards of an IS to support the accreditation process that establishes the extent to which a particular design and implementation meets a set of specified security requirements.

Certification authority (CA)

Third level of the Public Key Infrastructure (PKI) Certification Management Authority responsible for issuing and revoking user certificates, and exacting compliance to the PKI policy as defined by the parent Policy Creation Authority (PCA).

Certification package

Product of the certification effort documenting the detailed results of the certification activities.

Certification test and evaluation (CTE)

Software and hardware security tests conducted during development of an IS.

Certified TEMPEST technical authority (CTTA)

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

Certifier

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

Checksum

Value computed on data to detect error or manipulation during transmission. See hash total.

Ciphony

Process of enciphering audio information, resulting in encrypted speech.

Classified information

Information that has been determined pursuant to Executive Order 12958 or any predecessor Order, or by the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure and is marked to indicate its classified status.

Clearing

Removal of data from an IS, its storage devices, and other peripheral devices with storage capacity, in such a way that the data may not be reconstructed using common system capabilities (i.e., keyboard strokes); however, the data may be reconstructed using laboratory methods. Cleared media may be reused at the same classification level or at a higher level. Overwriting is one method of clearing.

Closed security environment

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

Command authority

Individual responsible for the appointment of user representatives for a department, agency, or organization and their key ordering privileges.

Common criteria

Provides a comprehensive, rigorous method for specifying security function and assurance requirements for products and systems. (Information Technology Security Evaluation Criteria [ITSEC])

Communications cove

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

Communications deception

Deliberate transmission, retransmission, or alteration of communications to mislead an adversary's interpretation of the communications. See imitative communications deception and manipulative communications deception.

Communications profile

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

Communications security (COMSEC)

Measures and controls taken to deny unauthorized persons information derived from telecommunications and to ensure the authenticity of such telecommunications.

Communications security includes cryptosecurity, transmission security, emission security, and physical security of COMSEC material.

Compartmentalization

A nonhierarchical grouping of sensitive information used to control access to data more finely than with hierarchical security classification alone. Compartmented mode INFOSEC mode of operation wherein each user with direct or indirect access to a system, its peripherals, remote terminals, or remote hosts has all of the following: (a) valid security clearance for the most restricted information processed in the system; (b) formal access approval and signed nondisclosure agreements for that information which a user is to have access; and (c) valid need-to-know for information which a user is to have access.

Compromise

Type of incident where information is disclosed to unauthorized persons or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred.

Compromising emanations

Unintentional signals that, if intercepted and analyzed, would disclose the information transmitted, received, handled, or otherwise processed by information systems equipment. See TEMPEST.

Computer abuse

Intentional or reckless misuse, alteration, disruption, or destruction of information processing resources.

Computer security

Measures and controls that ensure confidentiality, integrity, and availability of IS assets including hardware, software, firmware, and information being processed, stored, and communicated.

Computer security incident

See incident.

Computer security subsystem

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

COMSEC equipment

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

Concept of operations (CONOP)

Document detailing the method, act, process, or effect of using an IS.

Confidentiality

Assurance that information is not disclosed to unauthorized persons, processes, or devices.
Configuration control Process of controlling modifications to hardware, firmware, software, and documentation to ensure the IS is protected against improper modifications prior to, during, and after system implementation.

Configuration management

Management of security features and assurances through control of changes made to hardware, software, firmware, documentation, test, test fixtures, and test documentation throughout the life cycle of an IS. Confinement channel See covert channel.

Contamination

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

Contingency plan

Plan maintained for emergency response, backup operations, and post-disaster recovery for an IS, to ensure the availability of critical resources and to facilitate the continuity of operations in an emergency situation.

Controlled cryptographic item (CCI)

Secure telecommunications or information handling equipment, or associated cryptographic component, that is unclassified but governed by a special set of control requirements. Such items are marked "CONTROLLED CRYPTOGRAPHIC ITEM" or, where space is limited, "CCI."

Controlled security mode

See multilevel security.

Controlled sharing

Condition existing when access control is applied to all users and components of an IS.

Controlled space

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

Countermeasure

Action, device, procedure, technique, or other measure that reduces the vulnerability of an IS.

Covert channel

Unintended and/or unauthorized communications path that can be used to transfer information in a manner that violates an IS security policy. See overt channel and exploitable channel.

Covert channel analysis

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

Credentials

Information, passed from one entity to another, used to establish the sending entity's access rights.

Critical infrastructures

Those physical and cyber-based systems essential to the minimum operations of the economy and government.

CRYPTO

Marking or designator identifying COMSEC keying material used to secure or authenticate telecommunications carrying classified or sensitive U.S. Government or U.S. Government-derived information.

Crypto-equipment

Equipment that embodies a cryptographic logic.

Cryptography

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

Crypto-ignition key (CIK)

Device or electronic key used to unlock the secure mode of crypto-equipment.

D**Dangling threat**

Set of properties about the external environment for which there is no corresponding vulnerability and therefore no implied risk.

Dangling vulnerability

Set of properties about the internal environment for which there is no corresponding threat and, therefore, no implied risk.

Data aggregation

The compilation of unclassified individual data systems and data elements resulting in the totality of the information being classified.

Data flow control

Synonymous with information flow control.

Data integrity

Condition existing when data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed.

Data origin authentication

Corroborating the source of data is as claimed.

Data security

Protection of data from unauthorized (accidental or intentional) modification, destruction, or disclosure.

Decertification

Revocation of the certification of an IS item or equipment for cause. Dedicated mode IS security mode of operation wherein each user, with direct or indirect access to the system, its peripherals, remote terminals, or remote hosts, has all of the following: a. valid security clearance for all information within the system; b. formal access approval and signed

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

Default classification

Temporary classification reflecting the highest classification being processed in an IS. Default classification is included in the caution statement affixed to an object.

Denial of service

Type of incident resulting from any action or series of actions that prevents any part of an IS from functioning.

Designated approving authority(DAA)

Official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. This term is synonymous with designated accrediting authority and delegated accrediting authority.

Dial back

Synonymous with call back.

Digital signature

Cryptographic process used to assure message originator authenticity, integrity, and nonrepudiation.

Discretionary access control(DAC)

Means of restricting access to objects based on the identity and need-to-know of users and/or groups to which the object belongs. Controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (directly or indirectly) to any other subject. See mandatory access control.

Distinguished name

Globally unique identifier representing an individual's identity.

DoD Trusted Computer System Evaluation Criteria (TCSEC)

Document containing basic requirements and evaluation classes for assessing degrees of effectiveness of hardware and software security controls built into an IS. This document, DoD 5200.28 STD, is frequently referred to as the Orange Book.

Domain

Unique context (e.g., access control parameters) in which a program is operating; in effect, the set of objects a subject has the privilege to access.

Dominate

Term used to compare IS security levels. Security level S1 is said to dominate security level S2, if the hierarchical classification of S1 is greater than, or equal to, that of S2 and the non-hierarchical categories of S1 include all those of S2 as a subset.

E

Electronic Key Management System (EKMS)

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

Electronic messaging services

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

Electronic security(ELSEC)

Protection resulting from measures designed to deny unauthorized persons information derived from the interception and analysis of noncommunications electromagnetic radiations.

Embedded computer

Computer system that is an integral part of a larger system.

Embedded cryptography

Cryptography engineered into an equipment or system whose basic function is not cryptographic.

Emissions security

Protection resulting from measures taken to deny (EMSEC) unauthorized persons information derived from intercept and analysis of compromising emanations from crypto-equipment or an IS.

End-to-end security

Safeguarding information in an IS from point of origin to point of destination.

Endorsement

NSA approval of a commercially developed product for safeguarding national security information.

Entrapment

Deliberate planting of apparent flaws in an IS for the purpose of detecting attempted penetrations.

Environment

Aggregate of external procedures, conditions, and objects affecting the development, operation, and maintenance of an IS.

Erasure

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

Evaluated Products List (EPL)

Equipment, hardware, software, and/or firmware evaluated by the National Computer Security Center (NCSC) in accordance with DoD TCSEC and found to be technically compliant at a particular level of trust. The EPL is included in the NSA Information Systems Security Products and Services Catalogue.

Event

Occurrence, not yet assessed, that may effect the performance of an IS.

Executive state

One of several states in which an IS may operate, and the only one in which certain privileged instructions may be executed. Such privileged instructions cannot be executed when the system is operating in other states. Synonymous with supervisor state.

Exploitable channel

Channel that allows the violation of the security policy governing an IS and is usable or detectable by subjects external to the trusted computing base. See covert channel.

F**Fail safe**

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

Fail soft

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

Failure access

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

Failure control

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

Fetch protection

IS hardware provided restriction to prevent a program from accessing data in another user's segment of storage.

File protection

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

File security

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

FIREFLY

Key management protocol based on public key cryptography.

Firewall

System designed to defend against unauthorized access to or from a private network.

Firmware

Program recorded in permanent or semipermanent computer memory.

Flaw

Error of commission, omission, or oversight in an IS that may allow protection mechanisms to be bypassed.

Flaw hypothesis methodology

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

Flooding

Type of incident involving insertion of a large volume of data resulting in denial of service.

Formal access approval

Documented approval by a data owner allowing access to a particular category of information.

Formal development methodology

Software development strategy that proves security design specifications.

Formal security policy model

Mathematically precise statement of a security policy. Such a model must define a secure state, an initial state, and how the model represents changes in state. The model must be shown to be secure by proving the initial state is secure and all possible subsequent states remain secure.

Frequency hopping

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

Front-end security filter

Security filter logically separated from the remainder of an IS to protect system integrity. Synonymous with firewall.

Functional proponent

See network sponsor.

Functional testing

Segment of security testing in which advertised security mechanisms of an IS are tested under operational conditions.

G

Gateway

Interface providing a compatibility between networks by converting transmission speeds, protocols, codes, or security measures.

Granularity

Relative fineness to which an access control mechanism can be adjusted.

Guard

Process limiting the exchange of information between systems.

Gypsy verification environment

Integrated set of software tools for specifying, coding, and verifying programs written in the Gypsy language.

H

Hacker

Unauthorized user who attempts to or gains access to an IS.

Handshaking procedures

Dialogue between two IS's for synchronizing, identifying, and authenticating themselves to one another.

Hash total

Value computed on data to detect error or manipulation. See checksum.

Hashing

Computation of a hash total.

Hashword

Memory address containing hash total.

I

Identification

Process an IS uses to recognize an entity.

Identity token

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

Identity validation

Tests enabling an IS to authenticate users or resources.

Imitative communications deception

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

Impersonating

Form of spoofing.

Implant

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

Inadvertent disclosure

Type of incident involving accidental exposure of information to a person not authorized access.

Incident

(IS) Assessed occurrence having actual or potentially adverse effects on an IS.

(COMSEC) Occurrence that potentially jeopardizes the security of COMSEC material or the secure electrical transmission of national security Information or information governed by 10 U.S.C. Section 2315.

Incomplete parameter checking

System flaw that exists when the operating system does not check all parameters fully for accuracy and consistency, thus making the system vulnerable to penetration.

Indicator

A recognized action, specific, generalized, or theoretical, that an adversary might be expected to take in preparation for an attack.

Individual accountability

Ability to associate positively the identity of a user with the time, method, and degree of access to an IS.

Information assurance (IA)

Information operations that (IO) protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Information environment

Aggregate of individuals, organizations, or systems that collect, process, or disseminate information, also included is the information itself.

Information flow control

Procedure to ensure that information transfers within an IS are not made from a higher security level object to an object of a lower security level.

Information operations (IO)

Actions taken to affect adversary information and ISs while defending one's own information and ISs.

Information system (IS)

The entire infrastructure, organization, personnel, and components for the collection, processing, storage, transmission, display, dissemination, and disposition of information.

Information systems security (INFOSEC and/or ISS)

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

Information systems security engineering (ISSE)

Effort to achieve and maintain optimal security and survivability of a system throughout its life cycle.

Information systems security manager (ISSM)

Principal advisor on computer security matters.

Information systems security officer (ISSO)

Person responsible to the designated approving authority for ensuring the security of an Information system throughout its life cycle, from design through disposal. Synonymous with system security officer.

Information systems security product

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

Inspectable space

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

Integrity

Quality of an IS reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. Note that, in a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information.

Integrity check value

Checksum capable of detecting modification of an IS.

Interface

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

Interface control document

Technical document describing interface controls and identifying the authorities and responsibilities for ensuring the operation of such controls. This document is baselined during the preliminary design review and is maintained throughout the IS lifecycle.

Interim approval

Temporary authorization granted by a DAA for an IS to process information based on preliminary results of a security evaluation of the system.

Internal security controls

Hardware, firmware, or software features within an IS that restrict access to resources only to authorized subjects.

Internetwork private line interface

Network cryptographic unit that provides secure connections, singularly or in simultaneous multiple connections, between a host and a predetermined set of corresponding hosts.

Internet protocol (IP)

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

Intrusion

Unauthorized act of bypassing the security mechanisms of a system.

K

Key

Usually a sequence of random or pseudorandom bits used initially to set up and periodically change the operations performed in cryptoequipment for the purpose of encrypting or electronic counter-countermeasures patterns, or for producing other key.

Key distribution center (KDC)

COMSEC facility generating and distributing key in electrical form.

Key stream

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

L

Label

See security label.

Labeled security protections

Elementary-level mandatory access control protection features and intermediate-level discretionary access control features in a TCB that uses sensitivity labels to make access control decisions.

Laboratory attack

Use of sophisticated signal recovery equipment in a laboratory environment to recover information from data storage media.

Least privilege

Principle requiring that each subject be granted the most restrictive set of privileges needed for the performance of authorized tasks. Application of this principle limits the damage that can result from accident, error, or unauthorized use of an IS.

Level of protection

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

Line conditioning

Elimination of unintentional signals or noise induced or conducted on a telecommunications or IS signal, power, control, indicator, or other external interface line.

Line conduction

Unintentional signals or noise induced or conducted on a telecommunications or IS signal, power, control, indicator, or other external interface line.

List-oriented

IS protection in which each protected object has a list of all subjects authorized to access it. See also ticket-oriented.

Local authority

Organization responsible for generating and signing user certificates.

Lock and key protection system

Protection system that involves matching a key or password with a specific access requirement.

Logic bomb

Resident computer program triggering an unauthorized act when particular states of an IS are realized.

Logical completeness measure

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

Low probability of detection

Result of measures used to hide or disguise intentional electromagnetic transmissions.

Low probability of intercept

Result of measures to prevent the intercept of intentional electromagnetic transmissions.

M

Magnetic remanence

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

Maintenance hook

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

Malicious applets

Small application programs automatically downloaded and executed that perform an unauthorized function on an IS.

Malicious code

Software or firmware capable of performing an unauthorized process on an IS.

Malicious logic

Hardware, software, or firmware capable of performing an unauthorized function on an IS.

Mandatory access control(MAC)

Means of restricting access to objects based on the sensitivity of the information contained in the objects and the formal authorization (i.e., clearance, formal access approvals, and need-to-know) of subjects to access information of such sensitivity. See discretionary access control.

Manipulative communications deception

Alteration or simulation of friendly telecommunications for the purpose of deception. See communications deception and imitative communications deception.

Masquerading

Form of spoofing.

Memory scavenging

The collection of residual information from data storage.

Message authentication code

Data associated with an authenticated message allowing a receiver to verify the integrity of the message.

Message externals

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

Mimicking

Form of spoofing.

Mode of operation

Description of the conditions under which an IS operates based on the sensitivity of information processed and the clearance levels, formal access approvals, and need-to-know of its users. Four modes of operation are authorized for processing or transmitting information: dedicated mode, system high mode, compartmented/partitioned mode, and multilevel mode.

Multilevel device

Equipment trusted to properly maintain and separate data of different security categories.

Multilevel mode

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

Multilevel security (MLS)

Concept of processing information with different classifications and categories that simultaneously permits access by users with different security clearances and denies access to users who lack authorization.

Mutual suspicion

Condition in which two IS's need to rely upon each other to perform a service, yet neither trusts the other to properly protect shared data.

N

National security information (NSI)

Information that has been determined, pursuant to Executive Order 12958 or any predecessor order, to require protection against unauthorized disclosure.

National security system

Any telecommunications or information system operated by the United States Government, the function, operation, or use of which: 1. involves intelligence activities; 2. involves cryptologic activities related to national security; 3. involves command and control of military forces; 4. involves equipment that is an integral part of a weapon or weapon system; or 5. is critical to the direct fulfillment of military or intelligence missions and does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). (Title 40 U.S.C. Section 1452, Information Technology Management Reform Act of 1996.)

Need-to-know

The necessity for access to, or knowledge or possession of, specific information required to carry out official duties. Network IS implemented with a collection of interconnected nodes.

Network front-end

Device implementing protocols that allow attachment of a computer system to a network.

Network reference monitor

See reference monitor.

Network security

See information systems security.

Network security architecture

Subset of network architecture specifically addressing security-relevant issues.

Network security officer

See information systems security officer.

Network sponsor

Individual or organization responsible for stating the security policy enforced by the network, designing the network security architecture to properly enforce that policy, and ensuring the network is implemented in such a way that the policy is enforced.

Network system

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

Network trusted computing base(NTCB)

Totality of protection mechanisms within a network, including hardware, firmware, and software, the combination of which is responsible for enforcing a security policy. See trusted computing base.

Network trusted computing base (NTCB) partition

Totality of mechanisms within a single network component for enforcing the network policy, as allocated to that component; the part of the NTCB within a single network component.

Network weaving

Penetration technique in which different communication networks are linked to access an IS to avoid detection and trace-back.

Nonrepudiation

Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data.

Null

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

O

Object

Passive entity containing or receiving information. Access to an object implies access to the information it contains.

Object reuse

Reassignment and re-use of a storage medium containing one or more objects after ensuring no residual data remains on the storage medium.

Open storage

Storage of classified information within an accredited facility, but not in General Services Administration approved secure containers, while the facility is unoccupied by authorized personnel.

Operational data security (C.F.D)

Protection of data from either accidental or unauthorized intentional modification, destruction, or disclosure during input, processing, storage, transmission, or output operations.

Operations code

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

Operations security (OPSEC)

Process denying information to potential adversaries about capabilities and/or intentions by identifying, controlling, and protecting unclassified generic activities.

Orange Book(C.F.D)

The DoD Trusted Computer System Evaluation Criteria (DoD 5200.28-STD).

Organizational maintenance

Limited maintenance performed by a user organization.

Organizational registration authority (ORA)

Entity within the PKI that authenticates the identity and the organizational affiliation of the users.

Overt channel

Communications path within a computer system or network designed for the authorized transfer of data. See covert channel.

Overwrite procedure

Process of writing patterns of data on top of the data stored on a magnetic medium.

P

Parity

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

Partitioned security mode

IS security mode of operation wherein all personnel have the clearance, but not necessarily formal access approval and need-to-know, for all information handled by an IS.

Password

Protected/private alphanumeric string used to authenticate an identity or to authorize access to data.

Penetration

See intrusion.

Penetration testing

Security testing in which evaluators attempt to circumvent the security features of a system based on their understanding of the system design and implementation.

Periods processing

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

Plain text

Unencrypted information.

Policy approving authority (PAA)

First level of the PKI Certification Management Authority that approves the security policy of each PCA.

Policy certification authority (PCA)

Second level of the PKI Certification Management Authority that formulates the security policy under which it and its subordinate CAs will issue public key certificates.

Preproduction model

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

Print suppression

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

Privacy system

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

Privileged access

Explicitly authorized access of a specific user, process, or computer to a computer resource(s).

Probe

Type of incident involving an attempt to gather information about an IS for the apparent purpose of circumventing its security controls.

Production model

INFOSEC equipment in its final mechanical and electrical form.

Proprietary information

Material and information relating to or associated with a company's products, business, or activities, including but not limited to financial information; data or statements; trade secrets; product research and development; existing and future product designs and performance specifications; marketing plans or techniques; schematics; client lists; computer programs; processes; and know-how that have been clearly identified and properly marked by the company as proprietary information, trade secrets, or company confidential information. The information must have been developed by the company and not be available to the Government or to the public without restriction from another source.

Protection philosophy

Informal description of the overall design of an IS delineating each of the protection mechanisms employed. Combination of formal and informal techniques, appropriate to the evaluation class, used to show the mechanisms are adequate to enforce the security policy.

Protection ring

One of a hierarchy of privileged modes of an IS that gives certain access rights to user programs and processes that are authorized to operate in a given mode.

Protective packaging

Packaging techniques for COMSEC material that discourage penetration, reveal a penetration has occurred or was attempted, or inhibit viewing or copying of keying material prior to the time it is exposed for use.

Protective technologies

Special tamper-evident features and materials employed for the purpose of detecting tampering and deterring attempts to compromise, modify, penetrate, extract, or substitute information processing equipment and keying material.

Protocol

Set of rules and formats, semantic and syntactic, permitting IS's to exchange information.

Proxy

Software agent that performs a function or operation on behalf of another application or system while hiding the details involved.

Public cryptography (C.F.D.)

Body of cryptographic and related knowledge, study, techniques, and applications that is, or is intended to be, in the public domain.

Public key cryptography (PKC)

Encryption system using a linked pair of keys. What one key encrypts, the other key decrypts.

Public key infrastructure (PKI)

Framework established to issue, maintain, and revoke public key certificates accommodating a variety of security technologies, including the use of software.

Purging

Rendering stored information unrecoverable. See sanitize.

Q

R

Rainbow series (C.F.D.)

Set of publications that interpret Orange Book requirements for trusted systems.

Read

Fundamental operation in an IS that results only in the flow of information from an object to a subject.

Read access

Permission to read information in an IS.

Real time reaction

Immediate response to a penetration attempt that is detected and diagnosed in time to prevent access.

Recovery procedures

Actions necessary to restore data files of an IS and computational capability after a system failure.

RED

Designation applied to an IS, and associated areas, circuits, components, and equipment in which unencrypted national security information is being processed.

RED/BLACK concept

Separation of electrical and electronic circuits, components, equipment, and systems that handle national security information (RED), in electrical form, from those that handle non-national security information (BLACK) in the same form.

Red team

Independent and focused threat-based effort by an interdisciplinary simulated adversary to expose and exploit vulnerabilities as a means to improve the security posture of ISs.

RED signal

Any electronic emission (e.g., plain text, key, key stream, sub key stream, initial fill, or control signal) that would divulge national security information if recovered.

Reference monitor

Access control concept referring to an abstract machine that mediates all accesses to objects by subjects.

Reference validation mechanism

Portion of a trusted computing base whose normal function is to control access between subjects and objects and whose correct operation is essential to the protection of data in the system.

Remanence

Residual information remaining on storage media after clearing. See magnetic remanence and clearing.

Residual risk

Portion of risk remaining after security measures have been applied.

Residue

Data left in storage after information processing operations are complete, but before degaussing or overwriting has taken place.

Resource encapsulation

Method by which the reference monitor mediates accesses to an IS resource. Resource is protected and not directly accessible by a subject. Satisfies Requirement for accurate auditing of resource usage.

Risk

Possibility that a particular threat will adversely impact an IS by exploiting a particular vulnerability.

Risk analysis

Examination of information to identify the risk to an IS.

Risk assessment

Formal description and evaluation of risk to an IS.

Risk index

Difference between the minimum clearance or authorization of IS users and the maximum sensitivity (e.g., classification and categories) of data processed by the system.

Risk management

Process of identifying and applying countermeasures commensurate with the value of the assets protected based on a risk assessment.

S

Safeguarding statement

Statement affixed to a computer output or printout that states the highest classification being processed at the time the product was produced and requires control of the product, at that level, until determination of the true classification by an authorized person. Synonymous with banner.

Sanitize

Process to remove information from media such that data recovery is not possible. It includes removing all classified labels, markings, and activity logs. See purging.

Scavenging

Searching through object residue to acquire data.

Secure operating system (C.F.D.)

Resident software controlling hardware and other software functions in an IS to provide a level of protection or security appropriate to the classification, sensitivity, and/or criticality of the data and resources it manages.

Secure state

Condition in which no subject can access any object in an unauthorized manner.

Secure subsystem

Subsystem containing its own implementation of the reference monitor concept for those resources it controls. Secure subsystem must depend on other controls and the base operating system for the control of subjects and the more primitive system objects.

Security fault analysis(SFA)

Assessment, usually performed on IS hardware, to determine the security properties of a device when hardware fault is encountered.

Security features users guide(SFUG)

Guide or manual explaining how the security mechanisms in a specific system work.

Security filter

IS trusted subsystem that enforces security policy on the data passing through it.

Security flaw(C.F.D.)

Error of commission or omission in an IS that may allow protection mechanisms to be bypassed. See vulnerability.

Security inspection

Examination of an IS to determine compliance with security policy, procedures, and practices.

Security label

Information representing the sensitivity of a subject or object, such as its hierarchical classification (CONFIDENTIAL, SECRET, TOP SECRET) together with any applicable nonhierarchical security categories (e.g., sensitive compartmented information, critical nuclear weapon design information).

Security net control station

Management system overseeing and controlling implementation of network security policy.

Security perimeter

All components/devices of an IS to be accredited. Separately accredited components generally are not included within the perimeter.

Security policy

See information systems security policy.

Security range

Highest and lowest security levels that are permitted in or on an IS, system component, subsystem, or network.

Security requirements

Types and levels of protection necessary for equipment, data, information, applications, and facilities to meet IS security policy.

Security requirements baseline

Description of the minimum requirements necessary for an IS to maintain an acceptable level of security.

Security safeguards

Protective measures and controls prescribed to meet the security requirements specified for an IS. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. See accreditation.

Security specification

Detailed description of the safeguards required to protect an IS.

Security test and evaluation (STE)

Examination and analysis of the safeguards required to protect an IS, as they have been applied in an operational environment, to determine the security posture of that system.

Security testing

Process to determine that an IS protects data and maintains functionality as intended.

Sensitive information

Information, the loss, misuse, or unauthorized access to or modification of, which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under 5 U.S.C. Section 552a (the Privacy Act), but that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy. (Systems that are not national security systems, but contain sensitive information, are to be protected in accordance with the requirements of the Computer Security Act of 1987 (P.L.100-235).)

Sensitivity label

Information representing elements of the security label(s) of a subject and an object. Sensitivity labels are used by the trusted computing base (TCB) as the basis for mandatory access control decisions.

Shielded enclosure

Room or container designed to attenuate electromagnetic radiation.

Single-level device(C.F.D.)

IS device not trusted to properly maintain and separate data to different security levels.

Sniffer

Software tool for auditing and identifying network traffic packets.

Software system test and evaluation process

Process that plans, develops, and documents the quantitative demonstration of the fulfillment of all baseline functional performance, operational, and interface requirements.

Split knowledge

Separation of data or information into two or more parts, each part constantly kept under control of separate authorized individuals or teams so that no one individual or team will know the whole data.

Spoofing

Unauthorized use of legitimate Identification and authentication (IA) data, however it was obtained, to mimic a subject different from the attacker. Impersonating, masquerading, piggybacking, and mimicking are forms of spoofing.

Spread spectrum

Telecommunications techniques in which a signal is transmitted in a bandwidth considerably greater than the frequency content of the original information. Frequency hopping, direct sequence spreading, time scrambling, and combinations of these techniques are forms of spread spectrum.

State variable

Variable representing either the state of an IS or the state of some system resource.

Storage object

An object supporting both read and write accesses to an IS.

Subassembly

Major subdivision of an assembly consisting of a package of parts, elements, and circuits that perform a specific function.

Subject

Generally a person, process, or device causing information to flow among objects or change to the system state.

Subject security level

Sensitivity label(s) of the objects to which the subject has both read and write access. Security level of a subject must always be dominated by the clearance level of the user associated with the subject.

Supervisor state

Synonymous with executive state of an operating system.

Suppression measure

Action, procedure, modification, or device that reduces the level of, or inhibits the generation of, compromising emanations in an IS.

Surrogate access

See discretionary access control.

System administrator (SA)

Individual responsible for the installation and maintenance of an IS, providing effective IS utilization, adequate security parameters, and sound implementation of established INFOSEC policy and procedures.

System assets

Any software, hardware, data, administrative, physical, communications, or personnel resource within an IS.

System methodologies development

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

System high

Highest security level supported by an IS.

System high mode

IS security mode of operation wherein each user, with direct or indirect access to the IS, its peripherals, remote terminals, or remote hosts, has all of the following: a. valid security clearance for all information within an IS; b. formal access approval and signed nondisclosure agreements for all the information stored and/or processed (including all compartments, subcompartments and/or special access programs); and c. valid need-to-know for some of the information contained within the IS.

System integrity

Attribute of an IS when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

System low

Lowest security level supported by an IS.

System profile

Detailed security description of the physical structure, equipment component, location, relationships, and general operating environment of an IS.

System security

See information systems security.

System security engineering

See information systems security.

System security evaluation (C.F.D.)

Risk assessment of a system, considering its vulnerabilities and perceived security threat.

System security management plan (C.F.D.)

Formal document fully describing the responsibilities for security tasks planned to meet system security requirements.

System security officer

See information system security officer.

System security plan (C.F.D.)

Formal document fully describing the planned security tasks required to meet system security requirements.

T

Tampering

Unauthorized modification altering the proper functioning of INFOSEC equipment.

Telecommunications

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

Telecommunications security (TSEC)

See information systems security.

TEMPEST

Short name referring to investigation, study, and control of compromising emanations from IS equipment.

TEMPEST test

Laboratory or on-site test to determine the nature of compromising emanations associated with an IS.

TEMPEST zone

Designated area within a facility where equipment with appropriate TEMPEST characteristics (TEMPEST zone assignment) may be operated.

Threat

Any circumstance or event with the potential to adversely impact an IS through unauthorized access, destruction, disclosure, modification of data, and/or denial of service.

Threat analysis

Examination of information to identify the elements comprising a threat.

Threat assessment

Formal description and evaluation of threat to an IS.

Threat monitoring

Analysis, assessment, and review of audit trails and other information collected for the purpose of searching out system events that may constitute violations of system security.

Ticket-oriented

IS protection system in which each subject maintains a list of unforgeable bit patterns called tickets, one for each object a subject is authorized to access. See list-oriented.

Time bomb

Resident computer program that triggers an unauthorized act at a predefined time.

Time-compliance date

Date by which a mandatory modification to a COMSEC end-item must be incorporated if the item is to remain approved for operational use.

Time-dependent password

Password that is valid only at a certain time of day or during a specified interval of time.

Traditional COMSEC program

Program in which NSA acts as the central procurement agency for the development and, in some cases, the production of INFOSEC items. This includes the Authorized Vendor Program. Modifications to the INFOSEC end-items used in products developed and/or produced under these programs must be approved by NSA.

Traffic analysis (TA)

Study of communications patterns.

Traffic padding

Generation of spurious communications or data units to disguise the amount of real data units being sent.

Tranquility

Property whereby the security level of an object cannot change while the object is being processed by an IS.

Transmission security (TRANSEC)

Component of COMSEC resulting from the application of measures designed to protect transmissions from interception and exploitation by means other than cryptanalysis.

Trap door

Synonymous with back door.

Trojan horse

Program containing hidden code allowing the unauthorized collection, falsification, or destruction of information. See malicious code.

Trusted computer system

IS employing sufficient hardware and software assurance measures to allow simultaneous processing of a range of classified or sensitive information.

Trusted computing base (TCB)

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

Trusted distribution

Method for distributing trusted computing base (TCB) hardware, software, and firmware components that protects the TCB from modification during distribution.

Trusted identification forwarding

Identification method used in IS networks whereby the sending host can verify an authorized user on its system is attempting a connection to another host. The sending host transmits the required user authentication information to the receiving host.

Trusted path

Mechanism by which a person using a terminal can communicate directly with the trusted

computing base (TCB). Trusted path can only be activated by the person or the TCB and cannot be imitated by untrusted software.

Trusted process

Process that has privileges to circumvent the system security policy and has been tested and verified to operate only as intended.

Trusted recovery

Ability to ensure recovery without compromise after a system failure.

Trusted software

Software portion of a trusted computing base (TCB).

Tunneling

Technology enabling one network to send its data via another network's connections. Tunneling works by encapsulating a network protocol within packets carried by the second network.

U

Unauthorized disclosure

Type of event involving exposure of information to individuals not authorized to receive it.

Unclassified

Information that has not been determined pursuant to E.O. 12958 or any predecessor order to require protection against unauthorized disclosure and that is not designated as classified.

Untrusted process

Process that has not been evaluated or examined for adherence to the security policy. It may include incorrect or malicious code that attempts to circumvent the security mechanisms.

User

Person or process authorized to access an IS.

User ID

Unique symbol or character string used by an IS to identify a specific user.

User profile

Patterns of a user's activity that can show changes from normal behavior.

V

Validation

Process of applying specialized security test and evaluation procedures, tools, and equipment needed to establish acceptance for joint usage of an IS by one or more departments or agencies and their contractors.

Verification

Process of comparing two levels of an IS specification for proper correspondence (e.g., security policy model with top-level specification, top-level specification with source code, or source code with object code).

Verified design (C.F.D.)

Computer protection class in which formal security verification methods are used to assure mandatory and discretionary security controls can effectively protect classified and sensitive information stored in, or processed by, the system.

Virtual password (C.F.D.)

IS password computed from a pass phrase meeting the requirements of password storage (e.g., 64 bits).

Virtual private network (VPN)

Protected IS link utilizing tunneling, security controls (see information assurance), and endpoint address translation giving the impression of a dedicated line.

Virus

Self-replicating, malicious code that attaches itself to an application program or other executable system component and leaves no obvious signs of its presence.

Vulnerability

Weakness in an IS, system security procedures, internal controls, or implementation that could be exploited.

Vulnerability analysis

Examination of information to identify the elements comprising a vulnerability.

Vulnerability assessment

Formal description and evaluation of vulnerabilities of an IS.

W

Work factor

Estimate of the effort or time needed by a potential perpetrator, with specified expertise and resources, to overcome a protective measure.

Worm

See malicious code.

Write

Fundamental operation in an IS that results only in the flow of information from a subject to an object. See access type.

Write access

Permission to write to an object in an IS.

Z

Zero fill

To fill unused storage locations in an IS with the representation of the character denoting "0."

Zone of control

Synonymous with inspectable space.

