Annex A

Glossary of Acronyms and Terms

The discipline of computer security/IA is replete with acronyms and terminology. This annex defines these acronyms and terms as they are used in this book. Standardized definitions have been used wherever possible. When more than one standardized definition exists, multiple definitions are provided. When the legal and technical definitions of a term differ, both are provided. More complete definitions of IA analysis, design, verification, and accident/incident investigation techniques are given in Annex B: Glossary of Techniques.

Access control: Design feature(s) that protect IA-critical and IA-related systems, applications, and data by preventing unauthorized and unwarranted access to these resources.

Access control check: The security function that decides whether a subject's request to perform an action on a protected resource should be granted or denied.[216]

Accident: (1) Technical — any unplanned or unintended event, sequence, or combination of events that results in death, injury, or illness to personnel or damage to or loss of equipment or property (including data, intellectual property, etc.), or damage to the environment.[127,422,425] (2) Legal — any unpleasant or unfortunate occurrence that causes injury, loss, suffering, or death; an event that takes place without one's foresight or expectation.[214]

ACL: Access control list.

Activity monitor: Antiviral software that checks for signs of suspicious activity, such as attempts to rewrite program files, format disks, etc.[416]

AES: Advanced Encryption Standard, a new encryption standard, whose development and selection was sponsored by NIST, that will support key lengths of 128, 192, and 256 bits (see Reference 175).

AH: Authentication header.

ALARP: As low as reasonably practical; a method of correlating the likelihood of a hazard and the severity of its consequences to determine risk exposure acceptability or the need for further risk reduction.

Application proxy: A type of firewall that controls external access by operating at the application layer.[349] Application firewalls often readdress outgoing traffic so that it appears to have originated from the firewall rather than the internal host.[154]

AS: Authentication server; part of Kerberos KDC.

Assumption of risk: A plaintiff may not recover for an injury to which he assents; that is, that a person may not recover for an injury received when he voluntarily exposes himself to a known and appreciated danger. The requirements for the defense … are that: (1) the plaintiff has knowledge of facts constituting a dangerous condition, (2) he knows that the condition is dangerous, (3) he appreciates the nature or extent of the danger, and (4) he voluntarily exposes himself to the danger. Secondary assumption of risk occurs when an individual voluntarily encounters known, appreciated risk without an intended manifestation by that individual that he consents to relieve another of his duty.[214]

Audit trail: A set of records that collectively provides documentary evidence of system resources accessed by a user or process to aid in tracing from original transactions forward and backward to their component source transactions.

Authentication: To establish, verify, or prove the validity of a claimed identity of a user, process, or system.

Authentication header: An IPSec protocol that provides data origin authentication, packet integrity, and limited protection from replay attacks.

Authorization: Permission granted to access or use specific system resources or processes; access control privileges.

Availability: A measurement indicating the rate at which systems, data, and other resources are operational and accessible when needed, despite accidental and malicious intentional subsystem outages and environmental disruptions. Availability is usually defined as: MTBF/(MTBF + MTTR). However, this definition fails to take into account malicious intentional failures. (See expanded definition provided in Chapter 6.)

Backdoor: A function built into a program or system that allows unusually high or even full access to the system, either with or without an account in a normally restricted account environment. The backdoor sometimes remains in a fully developed system either by design or accident.[416] (*See also* trap door.)

Bayesian Belief network: Graphical networks that represent probabilistic relationships among variables. The nodes represent uncertain variables and the arcs represent the causal/relevance relationships between the variables. The probability tables for each node provide the probabilities of each state of the variable for that node, conditional on each combination of values of the parent node.[431]

BBN: Bayesian Belief network.

Biometric system: A pattern recognition system that establishes the authenticity of a specific physiological or behavioral characteristic possessed by a user.[374]

BIT: Built-in test.

Block ciphers: Encryption algorithms that operate on a fixed number of bits of data at a time, known as the blocksize. For example, DES operates on 64-bit (8-byte) blocks of data. Contrast with stream ciphers.

Brute-force attack: A form of cryptoanalysis where the attacker uses all possible keys or passwords in an attempt to crack an encryption scheme or login system.[349]

BSP: Biometric service provider.

Built-in test: A design feature that provides information on the ability of the item to perform its intended functions. BIT is implemented in software or firmware and may use or control BIT equipment (BITE).[127]

C&A: Certification and accreditation; a comprehensive evaluation of the technical and nontechnical security features of a system to determine if it meets specified requirements and should receive approval to operate.

CA: Certificate authority.

Cause: (1) Technical — the action or condition by which a hazardous event (physical or cyber) is initiated — an initiating event. The cause may arise as the result of failure, accidental or intentional human error, design inadequacy, induced or natural environment, system configuration, or operational modes/states.[31] (2) Legal — each separate antecedent of an event. Something that precedes and brings about an effect or result. A reason for an accident or condition.[214]

CBEFF: Common biometric exchange file format; being defined by U.S. biometric consortium and ANSI X9F4 subcommittee.

CBC: Cipher block chaining.

CC: Common Criteria; *see* ISO/IEC 15408.

CCF: Common cause failure.

CEPS: Common electronic purse specifications; a standard used with smartcards.

CERT/CC: Computer emergency response team coordination center, a service of CMU/SEI.

Certificate authority: A trusted third party that associates a public key with proof of identity by producing a digitally signed certificate.[349]

CGI: Common gateway interface.

CHAP: Challenge handshake authentication protocol.

Challenge handshake authentication protocol: A secure login procedure for dial-in access that avoids sending in a password in the clear by using cryptographic hashing.

CIDF: Common intrusion detection framework model.

Cipher text: A message that has been encrypted using a specific algorithm and key. (Contrast with plain text.)

CISL: Common Intrusion Specification Language.

CMF: Common mode failure.

Cohesion: The manner and degree to which the tasks performed by a single software module are related to another. Types of cohesion include coincidental, communication, functional, logical, procedural, sequential, and temporal.[44,127]

Common cause failure: Failure of multiple independent system components occurring from a single cause that is common to all of them.[31]

Common mode failure: Failure of multiple independent system components that fail in the identical mode.[31]

Communications security: A collection of engineering activities that are undertaken to protect the confidentiality, integrity, and availability of sensitive data while it is being transmitted between systems and networks.

Compromise: An unwarranted and uninvited offensive incursion, infringement, or encroachment of a system, usually by stealth, that defeats safety and security mechanisms to violate and usurp resources and data in a hostile and injurious manner.

COMPUSEC: Computer security.

Computer security: Preventing, detecting, and minimizing the consequences of unauthorized actions by users (authorized and unauthorized) of a computer system.

COMSEC: Communications security.

Confidentiality: The characteristic of information being disclosed by or made available only to authorized entities at authorized times and in the approved manner.[189] Confidentiality does not guarantee integrity.[433]

Confinement: (1) Confining an untrusted program so that it can do everything it needs to do to meet the user's expectation, but nothing else.[335] (2) Restricting an untrusted program from accessing system resources and executing system processes. Common confinement techniques include DTE, least privilege, and wrappers.

Contingency plan: Providing a planned measured response to the sudden loss, unavailability, or anomalous performance of one or more system entities, whether internal or external, in order to quickly return the system to a known safe and secure state.

Continuous-mode operation: Systems that are operational continuously, 24 hours a day, 7 days a week.

Controllability: The ability to control the situation following a failure. (Note that controllability has a different meaning when used in the context of testability analysis.)

Controlled security mode: A system is operating in the controlled security mode when at least some users with access to the system have neither a security clearance nor a need-to-know for all classified material contained in the system. However, the separation and control of users and classified material on the basis, respectively, of security clearance and security classification are not essentially under operating system control as in the multilevel security mode.[140]

CORBAsecurity: The Object Management Group standard that describes how to secure CORBA environments.

Coupling: The manner and degree of interdependence between software modules. Types include common environment coupling, content coupling, control coupling, data coupling, hybrid coupling, and pathological coupling.[44,127]

Countermeasure: *See* threat control measure.

Covert channel: (1) A communications channel that allows a process to transfer information in a manner that violates the system's security policy.[140] (2) An information flow that is not controlled by a security mechanism.[120–122]

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 that is shared by two subjects at different security levels.[140]

Covert timing channel: A covert channel in which one process signals information to another by modulating its own use of system resources in such a way that this manipulation affects the real response time observed by the second process.[140]

Critical software: A defined set of software components that have been evaluated and whose continuous operation has been determined essential for safe, reliable, and secure operation of the system. Critical software is composed of three elements: (1) safety-critical and safety-related software, (2) reliability-critical software, and (3) security-critical software.[32]

CRL: Certificate revocation list.

Cross certificate: A certificate issued by a certificate authority in one domain whose subject resides in another domain, the purpose of which is to enable different domains to convey trust in each other so that they can interoperate.

Cryptography: The science of transforming messages for the purpose of making the message unintelligible to all but the intended receiver.[249]

CSI: Computer Security Institute.

DAC: Discretionary access controls.

Damage: Loss, injury, or deterioration caused by the negligence, design, or accident of one person to another, in respect of the latter's person or property; the harm, detriment, or loss sustained by reason of an injury.[214]

DASS: Distributed authentication security service.

Data integrity: The state that exists when computerized data is the same as that in the source information and has not been exposed to accidental or malicious addition, alteration, or destruction.

Data safety: Ensuring that: (1) the intended data has been correctly accessed, (2) the data has not been manipulated or corrupted intentionally or accidentally, and (3) the data is legitimate.[288]

Deadlock: A situation in which computer processing is suspended because two or more devices or processes are each awaiting resources assigned to the other.[127]

Dedicated security mode: A system is operating in the dedicated security mode when the system and all of its local and remote peripherals are exclusively used and controlled by specific users or groups of users who have a security clearance and need-to-know for the processing of a particular category and type of classified material.[140]

Defect: Deficiency; imperfection; insufficiency; the absence of something necessary for completeness or perfection; a deficiency in something essential to the proper use for the purpose for which a thing is to be used; a manufacturing flaw, a design defect, or inadequate warning.[214]

Defense in depth: Provision of several overlapping subsequent limiting barriers with respect to one safety or security threshold, so that the threshold can only be surpassed if all barriers have failed.[60]

Defensive programming: Designing software that detects anomalous control flow, data flow, or data values during execution and reacts in a predetermined and acceptable manner. The intent is to develop software that correctly accommodates design or operational shortcomings; for example, verifying a parameter or command through two diverse sources before acting upon it.[68]

Degraded-mode operation: Maintaining the availability of the more critical system functions, despite failures, by dropping the less critical functions. Also referred to as graceful degradation.[68]

Demand-mode operation: Systems that are used periodically on-demand; for example, a computer-controlled braking system in a car.

Denial of service: (1) Prevention of authorized access to resources or the delaying of time-critical operations.[120–122] (2) Sending a series of e-mail, connection requests, etc. to the target system with the intent of inducing saturation.

Dependability: That property of a computer system such that reliance can be justifiably placed on the service it delivers. The service delivered by a system is its behavior as it is perceived by its user(s); a user is another system or human that interacts with the former.[390]

DES: Data encryption standard; *see* FIPS PUB 46-3.[155]

DIAP: Defense-wide IA program (U.S. DoD).

Digital certificate: A document containing public-key material combined with fields identifying the owner and issuer of the certificate. The CA digitally signs the document to ensure validity of the contents.[349]

Digital signature: (1) A string of characters that can be generated only by an agent that knows some secret and hence provides evidence that such an agent must have generated it.[362] (2) A block of data attached to a message or document that binds the data to a particular individual or entity so that it can be verified by the receiver or an independent third party.[248]

DII: Defense information infrastructure.

Discretionary access controls: A non-policy-based means of restricting access to objects based on the identity of subjects 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.

DITSCAP: U.S. DoD IT Security Certification and Accreditation Process.

Diversity: Using multiple different means to perform a required function or solve the same problem. Diversity can be implemented in software and hardware.

Domain: The set of objects that a subject (user or process) has the ability to access.

Domain and type enforcement: A confinement technique in which an attribute called a domain is associated with each subject and another attribute called a type is associated with each object. A matrix specifies whether a particular mode of access to objects of a type is granted or denied to subjects in a domain.[335]

DSS: Digital signature standard; *see* FIPS PUB 186.[165]

DSSA: Distributed system security architecture; developed by Digital Equipment Corporation.

DTE: Domain and type enforcement.

Dynamic analysis: Exercising the system being assessed through actual execution; includes exercising the system functionally (traditional testing) and logically through techniques such as failure assertion, structural testing, and statistical-based testing. Major system components have to have been built before dynamic analysis can be performed.

EAL: Evaluation assurance level.

EAP: Extensible Authentication Protocol.

EMC: Electromagnetic conductance.

EMI: Electromagnetic interference.

Encapsulated Security Payload: An IPSec protocol that provides confidentiality, data origin authentication, data integrity services, tunneling, and protection from replay attacks.

Encapsulation: *See* wrappers.

Encryption: (1) Symmetric — a systematic method of scrambling information to provide confidentiality using secret keys for encryption and decryption. (2) Asymmetric — a systematic method of scrambling information to provide confidentiality using one key to encrypt messages and one key to decrypt messages. The two keys, referred to as public and private keys, only work in designated pairs. Encryption can be implemented in hardware or software with block or stream ciphers.

Error: The difference between a computed, observed, or measured value or condition and the true, specified, or theoretically correct value or condition.[44]

Error of commission: An error that results from making a mistake or doing something wrong.

Error of omission: An error that results from something that was not done.

ESP: Encapsulated Security Payload protocol.

Evaluation assurance level: One of seven levels defined by the Common Criteria[52,120–122] that represent the degree of confidence that specified functional security requirements have been met by a commercial product.

Extensible Authentication Protocol: An IETF standard means of extending authentication protocols, such as CHAP and PAP, to include additional authentication data; for example, biometric data.[349]

Fail operational: The system must continue to provide some degree of service if it is not to be hazardous; it cannot simply shut down — for example, an aircraft flight control system.[345] (*See* degraded-mode operation.)

Fail safe/secure: (1) A design wherein the component/system, should it fail, will fail to a safe/secure condition.[425] (2) The system can be brought to a safe/secure condition or state by shutting it down; for example, the shutdown of a nuclear reactor by a monitoring and protection system.[345]

Failure: Failing to or inability of a system, entity, or component to perform its required function(s), according to specified performance criteria, due to one or more fault conditions. Three categories of failure are commonly recognized**:** (1) incipient failures are failures that are about to occur; (2) hard failures are failures that result in a complete shutdown of a system; and (3) soft failures are failures that result in a transition to degraded-mode operations or a fail operational status.[44]

Failure minimization: Actions designed or programmed to reduce failure possibilities to the lowest rates possible.[425]

Fault: A defect that results in an incorrect step, process, data value, or mode/state.

Fault tolerance: Built-in capability of a system to provide continued correct execution in the presence of a limited number of hardware or software faults.[60]

FedCIRC: The U.S. federal government Computer Incident Response Center; managed by the General Services Administration (GSA).

Firewall: A security gateway between two networks that uses a variety of techniques, such as proxy filters, packet filters, application level gateways, and circuit level gateways, to block unwanted users, processes, and data while protecting legitimate users and sensitive data and processes.

Flooded transmission: A transmission in which data is sent over every link in the network.

FMECA: Failure mode effects criticality analysis; an IA analysis technique that systematically reviews all components and materials in a system or product to determine cause(s) of their failures, the downstream results of such failures, and the criticality of such failures as accident precursors. FMECA can be performed on individual components (hardware, software, and communications equipment) and integrated at the system level. *See* IEC 60812(1985).

Formal design: The part of a software design written using a formal notation.[129]

Formal method: (1) A software specification and production method, based on discrete mathematics, that comprises: a collection of mathematical notations addressing the specification, design, and development processes of software production, resulting in a well-founded logical inference system in which formal verification proofs and proofs of other properties can be formulated, and a methodological framework within which software can be developed from the specification in a formally verifiable manner.[129] (2) The use of mathematical techniques in the specification, design, and analysis of computer hardware and software.[422]

Formal notation: The mathematical notation of a formal method.[129]

Formal proof: The discharge of a proof obligation by the construction of a complete mathematical proof.[129]

Formal specification: The part of the software specification written using a formal notation.[129]

FTA: Fault tree analysis; an IA analysis technique by which possibilities of occurrence of specific adverse events are investigated. All factors, conditions, events, and relationships that could contribute to that event are analyzed.[425] FTA can be performed on individual components (hardware, software, and communications equipment) and integrated at the system level. *See* IEC 61025(1990).

FTP: File Transfer Protocol; an application layer protocol.

Functional safety: The ability of a safety-related system to carry out the actions necessary to achieve or maintain a safe state for the equipment under control.[65]

GII: Global information infrastructure.

GPKI: Global public key infrastructure.

Graceful degradation: *See* degraded-mode operation.

Guard: A component that mediates the flow of information or control between different systems or networks.[362]

HAG: High assurance guard.

Hardware reliability: The ability of an item to correctly perform a required function under certain conditions in a specified operational environment for a stated period of time.

Hardware safety integrity: The overall failure rate for continuous-mode operations and the probability to operate on demand for demand-mode operations relative to random hardware failures in a dangerous mode of failure.[69]

Hazard: A source of potential harm or a situation with potential to harm.[56] Note that the consequences of a hazard can be physical or cyber.

Hazard likelihood: The qualitative or quantitative likelihood that a potential hazard will occur. Most international standards define six levels of hazard likelihood (lowest to highest): incredible, improbable, remote, occasional, probable, and frequent.

Hazard severity: The severity of the worst-case consequences should a potential hazard occur. Most international standards define four levels of hazard severity (lowest to highest): insignificant, marginal, critical, and catastrophic.

HAZOP: Hazard and operability study; a method of determining hazards in a proposed or existing system, their possible causes and consequences, and recommending solutions to minimize the likelihood of occurrence. Design and operational aspects of the system are analyzed by an interdisciplinary team.[69]

HTTP: Hypertext Transfer Protocol; an application layer protocol.

I&A: Identification and authentication.

IA: Information assurance.

IA-critical: A term applied to any condition, event, operation, process, or item whose proper recognition, control, performance, or tolerance is essential to the safe, reliable, and secure operation and support of a system.

IA integrity: The likelihood of a system, entity, or function achieving its required security, safety, and reliability features under all stated conditions within a stated measure of use.[130]

IA integrity case: A systematic means of gathering, organizing, analyzing, and reporting the data needed by internal, contractual, regulatory, or Certification Authorities to confirm that a system has met the specified IA goals and IA integrity level and is fit for use in the intended operational environment. An IA integrity case includes assumptions, claims, and evidence.

IA integrity level: The level of IA integrity that must be achieved or demonstrated to maintain the IA risk exposure at or below its acceptable level.

IA-related: A system or entity that performs or controls functions which are activated to prevent or minimize the effect of a failure of an IA-critical system or entity.

ICSA: Internet Computer Security Association.

IDS: Intrusion detection system.

IETF: Internet Engineering Task Force; a public consortium that develops standards for the Internet.

IKE: Internet Key Exchange protocol.

Incident: Any unplanned or unintended event, sequence, or combination of events that does not result in death, injury, or illness to personnel or damage to or loss of equipment or property (including data, intellectual property, etc.) or damage to the environment, but has the potential to do so; a near-miss.

Information assurance: (1) An engineering discipline that provides a comprehensive and systematic approach to ensuring that individual automated systems and dynamic combinations of automated systems interact and provide their intended functionality, no more and no less, safely, reliably, and securely in the intended operational environment(s). (2) Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation; including providing for restoration of information systems by incorporating protection, detection, and reaction capabilities (DoD Directive 5-3600.1).

Information hiding: (1) A software development technique in which each module's interfaces reveal as little as possible about the module's inner workings and other modules are prevented from using information about the module that is not in the module's interface specification.[18] (2) A software development technique that consists of isolating a system function, or set of data and operations on those data, within a module and providing precise specifications for the module.[69]

INFOSEC: (1) The combination of COMSEC and COMPUSEC — the protection of information against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional. (2) Protection of information

systems against unauthorized access to or modification of information, whether in storage, processing, or transit, and against denial of service to authorized users, including those measures necessary to detect, document, and counter such threats.[154]

Infrastructure system: A network of independent, mostly privately owned, automated systems and processes that function collaboratively and synergistically to produce and distribute a continuous flow of essential goods and services.[176,178] The eight critical infrastructure systems defined by PDD-63 are: telecommunications, banking and finance, power generation and distribution, oil and gas distribution and storage, water processing and supply, transportation, emergency services, and government services.[178]

Inhibit: A design feature that provides a physical interruption between an energy source and a function actuator. Two inhibits are independent if no single failure can eliminate them both.[28,127]

Injury: Any wrong or damage done to another, either his person, rights, reputation, or property; the invasion of any legally protected interest of another.[214]

Integrity level: (1) A range of values of an item necessary to maintain system risks within acceptable limits. For items that perform IA-related mitigating functions, the property is the reliability with which the item must perform the mitigating function. For IA-critical items whose failure can lead to threat instantiation, the property is the limit on the frequency of that failure.[58] (2) A range of values of a property of an item necessary to maintain risk exposure at or below its acceptability threshold.[48]

Intelligent transportation systems: A subset or specific application of the NII that provides real-time information and services to the transportation sector. Specific examples include: travel and transportation management systems, travel demand management systems, public transportation operation systems, electronic payment systems, commercial vehicle operation systems, emergency management systems, and advanced vehicle control and safety systems.[224]

Internetwork: A group of networks connected by routers so that computers on different networks can communicate; the Internet.

Intrusion detection: Recognition of a security breach, either as it is happening or immediately afterward.[433]

IO: Information operations.

IP: Internet Protocol.

IPC: Inter-process communication.

IPSec: The security architecture for IP; developed by the IETF to support reliable and secure datagram exchange at the IP layer. The IPSec architecture specifies AH, ESP, Internet Key Exchange (IKE), and Internet Security Association Key Management Protocol (ISAKMP), among other things.

IP spoofing: An intruder fakes his IP address to masquerade as a trusted host during address-based authentication.[372]

ISAKMP: Internet Security Association Key Management Protocol.

ISSA: Information Systems Security Association.

ITS: Intelligent transportation systems.

IW: Information warfare.

KDC: Key distribution center.

Kerberos: A network authentication product that also provides a confidentiality service.

KMI: Key management infrastructure.

Least privilege: Confinement technique in which each process is given only the minimum privileges it needs to function; also referred to as sandboxing. (*See also* need-to-know.)

Letter bomb: A Trojan horse that will trigger when an e-mail message is read.

Liability: Condition of being or potentially subject to an obligation; condition of being responsible for a possible or actual loss, penalty, evil, expense, or burden. Condition that creates a duty to perform an act immediately or in the future, including almost every character of hazard or responsibility, absolute, contingent, or likely.[214]

Logic bomb: A Trojan horse that will trigger when a specific logical event or action occurs.

LRA: Local registration authority (for digital certificates).

MAC: (1) Mandatory access controls. (2) Message authentication codes. (3) Media access control.

Mandatory access controls: A policy-based 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 (access control privileges) of subjects to access information of such sensitivity.

Man-in-the-middle attack: Scenarios in which a malicious user can intercept messages and insert other messages that compromise the otherwise secure exchange of information between two parties.[349]

Mediation: Action by an arbiter that decides whether or not a subject or process is permitted to perform a given operation on a specified object.

Message authentication codes: A value computed from the message and a secret cryptographic key to provide assurance about the source and integrity of a message; also referred to as keyed hash functions.

Mishap risk: An expression of the possibility and impact of an unplanned event or series of events resulting in death, injury, occupational illness, damage to or loss of equipment or property (physical or cyber), or damage to the environment in terms of potential severity of consequences and likelihood of occurrence.[143] (*See also* risk.)

MISPC: Minimum interoperability specification of PKI components; a standard that specifies a minimal set of features, transactions, and data formats for the various certification management components that make up a PKI.

Mistake: An erroneous human action (accidental or intentional) that produces a fault condition.

MLS: Multi-level secure.

MNWF: Must not work function.

Multi-level secure: A class of systems 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.

Must not work function: Sequences of events or commands that are prohibited because they would result in a system hazard.[126,127]

Must work function: Software that if not performed or performed incorrectly, inadvertently, or out of sequence could result in a hazard or allow a hazardous condition to exist. This includes (1) software that directly exercises command and control over potentially hazardous functions or hardware; (2) software

that monitors critical hardware components; and (3) software that monitors the system for possible critical conditions or states.[126,127]

MWF: Must work function.

National information infrastructure: The total interconnected national telecommunications network of a country, which is made up of the private lines of major carriers, numerous carriers and interconnection companies, and thousands of local exchanges that connect private telephone lines to the national network and the world.[279]

NCSA: National Computer Security Association; superseded by ICSA.

NCSC: National Computer Security Center; part of the U.S. Department of Defense.

Need-to-know: A method of isolating information resources based on a user's need to have access to that resource in order to perform their job but no more; for example, a personnel officer needs access to sensitive personnel records and a marketing manager needs access to sensitive marketing information but not vice versa. The terms "need-to-know" and "least privilege" express the same idea. Need-to-know is generally applied to people, while least privilege is generally applied to processes.

Negligence: Failure to use such care as a reasonably prudent and careful person would use under similar circumstances; the doing of some act which a person of ordinary prudence would not have done under similar circumstances or failure to do what a person of ordinary prudence would have done under similar circumstances; conduct that falls below the norm for the protection of others against unreasonable risk of harm. It is characterized by inadvertence, thoughtlessness, inattention, recklessness, etc.[214]

Network sink: A router that drops or misroutes packets, accidentally or on purpose. Intelligent network sinks can cooperate to conceal evidence of packet dropping.

NIAP: Joint industry/government (U.S.) National IA Partnership.

NII: National information infrastructure of a specific country.

NIPC: U.S. National Infrastructure Protection Center.

NLS: Network Layer Security Protocol.

Noninterference: The property that actions performed by user or process A of a system have no effect on what user or process B can observe; there is no information flow from A to B.[255]

Nonrepudiation: A security service by which evidence is maintained so that the sender and recipient of data cannot deny having participated in the communication.[154] Referred to individually as nonrepeduation of origin and nonrepudiation of receipt.

Operational error: An error that results from the incorrect use of a product, component, or system.

Operational profile: The set of operations that the software can execute along with the probability with which they will occur.[343]

Operations security: The implementation of standardized operational security procedures that define the nature and frequency of the interaction between users, systems, and system resources, the purpose of which is to (1) maintain a system in a known secure state at all times, and (2) prevent accidental or intentional theft, destruction, alteration, or sabotage of system resources.

OPSEC: Operations security.

OSI: Open Systems Interconnection; a seven-layer model from the ISO that defines and standardizes protocols for communicating between systems, networks and devices. (*See* the standards listed in Section C.1 of Annex C.)

PAP: Password Authentication Protocol.

Partitioning: Isolating IA-critical, IA-related, and non-IA-related functions and entities to prevent accidental or intentional interference, compromise, and corruption. Partitioning can be implemented in hardware or software. Software partitioning can be logical or physical. Partitioning is often referred to as separability in the security community.

Password: A private character string that is used to authenticate an identity.

Password sniffing: Eavesdropping on a communications line to capture passwords that are being transmitted unencrypted.[372]

PDU: Protocol data unit.

PEM: Privacy Enhanced Mail; an e-mail encryption protocol.

Pest program: Collective term for programs with deleterious and generally unanticipated side effects; for example, Trojan horses, logic bombs, letter bombs, viruses, and malicious worms.[362]

PGP: Pretty Good Privacy; an e-mail and file encryption protocol.

Physical security: Protection of hardware, software, and data against physical threats, to reduce or prevent disruptions to operations and services and loss of assets.

PKI: Public key infrastructure.

Plain text: A message before it has been encrypted or after it has been decrypted using a specific algorithm and key; also referred to as clear text. (Contrast with cipher text.)

PP: Protection profile.

Privacy: The rights of individuals and organizations to determine for themselves when, how, and to what extent information about them is to be transmitted to others.[344] Privacy concerns transcend the boundaries of automated systems.

Private key: In a public-key asymmetric cryptosystem, the private key counterpart of a public key; the key that is private to the owner and does not need to be shared.[362]

Public key: In a public-key asymmetric cryptosystem, the public key counterpart of a private key; the key that is public and does not need to be protected.[362]

Public key cryptosystem: An asymmetric cryptosystem that uses a public key and a corresponding private key.[362]

Public key infrastructure: A network of services that includes certificate authorities, certificate repositories, and directory services for storing and finding public key certificates, and certificate revocation lists for managing keys that expire or are revoked.[248]

Qualitative: Inductive analytical approaches that are oriented toward relative, nonmeasurable, and subjective values, such as expert judgment.[425]

Quantitative: Deductive analytical approaches that are oriented toward the use of numbers or symbols to express a measurable quantity, such as MTTR.[425]

RADIUS: Remote Authentication Dial-In User Service.

Random failure: Failures that result from physical degradation over time and variability introduced during the manufacturing process.

Recognition: Capability to detect attacks as they occur and to evaluate the extent of damage and compromise.[336]

Recovery: The ability to maintain essential services and assets during an attack, limit the extent of damage, and restore full services following an attack.[336]

Redundancy: Controlling failure by providing several identical functional units, monitoring the behavior of each to detect faults, and initiating a transition to a safe/secure condition if a discrepancy is detected.[69]

Reference monitor: (1) An access control concept that refers to an abstract machine that mediates all accesses to objects by subjects.[135,141] (2) A system component that mediates usage of all objects by all subjects, enforcing the intended access controls.[362]

Reliability critical: A term applied to any condition, event, process, or item whose recognition, control, performance or tolerance is essential to reliable system operation or support.

Remote Authentication Dial-In User Service: An IETF standard protocol that supports authentication, management, and accounting for remote and dial-in users.[349]

Residual risk: The risk that remains after threat control measures have been employed. Before a system can be certified, a determination must be made about the acceptability of residual risk.

Residue: Accessible vestiges of de-allocated resources, such as memory.

Resistance: Capability of a system to repel attacks.[336]

RFI: Radio frequency interference.

Risk: A combination of the likelihood of a hazard occurring and the severity of the consequences should it occur. (*See also* mishap risk.)

Risk analysis: A series of analyses conducted to identify and determine the cause(s), consequences, likelihood, and severity of hazards. Note that a single hazard may have multiple causes.

Risk control: Techniques that are employed to eliminate, reduce, or mitigate risk, such as inherent safe and secure (re)design techniques/features, alerts, warnings, operational procedures, instructions for use, training, and contingency plans.

Risk dimension: *See* threat perspective.

Risk exposure: The exposure to loss presented to an organization or individual by a risk; the product of the likelihood that the risk will occur and the magnitude of the consequences of its occurrence.[48]

Risk management: Systematic application of risk analysis and risk control management policies, procedures, and practices.

Root cause: Underlying cause(s), event(s), conditions, or actions that individually or in combination led to the accident/incident; primary precursor event(s) that have the potential for being corrected.

RSA: Rivest-Shamir-Adelman public key encryption algorithm; *see* PKCS #1.[179]

S/MIME: Secure Multipurpose Internet Mail Extensions; an e-mail and file encryption protocol.

Safety-critical: A term applied to any condition, event, operation, process, or item whose proper recognition, control, performance, or tolerance is essential to safe system operation and support (such as a safety-critical function, safety-critical path, or safety-critical component.[143]

Safety-critical software: Software that performs or controls functions which, if executed erroneously or if they failed to execute properly, could directly inflict serious injury to people, property, or the environment or cause loss of life.[288]

Safety integrity: (1) The likelihood of a safety-related system, function, or component achieving its required safety features under all stated conditions within a stated measure of use.[130] (2) The probability of a safety-related system satisfactorily performing the required safety functions under all stated conditions within a stated period of time.[65]

Safety integrity level: An indicator of the required level of safety integrity; the level of safety integrity that must be achieved and demonstrated.

Safety kernel: An independent computer program that monitors the state of the system to determine when potentially unsafe system states may occur or when transitions to potentially unsafe system states may occur. A safety kernel is designed to prevent a system from entering an unsafe state and retaining or returning it to a known safe state.[126,127,435]

Safety-related software: Software that performs or controls functions that are activated to prevent or minimize the effect of a failure of a safety-critical system.[288]

Sanitization: (1) Removing the classified content of an otherwise unclassified resource. (2) Removing any information that could identify the source from which the information came.

Secure Electronic Transactions protocol: Used in conjunction with SSL3 and TLS1 to encrypt credit card information so that only the customer and their bank see it, but not the merchant.

Secure Socket Layer: Internet protocol used to protect credit card numbers and other sensitive data between a Web browser and a Web server; developed by Netscape Communications. (*See also* TLS1.)

Security: (1) Freedom from undesirable events, such as malicious and accidental misuse; how well a system resists penetrations by outsiders and misuse by insiders.[362] (2) The protection of system resources from accidental or malicious access, use, modification, destruction, or disclosure.[58] (3) The protection of resources from damage and the protection of data against accidental or intentional disclosure to unauthorized persons or unauthorized modifications or destruction.[344] Security concerns transcend the boundaries of an automated system.

Security association: The keying material and set of mechanisms (cryptographic algorithms, hashing functions, etc.) agreed upon by two entities that will be used to protect and authenticate communications.

Security-critical: A term applied to any condition, event, process, or item whose recognition, control, performance, or tolerance is essential to secure system operation or support.

Security kernel: The hardware, firmware, and software elements of a trusted computing base that implement the reference monitor concept. It must mediate all accesses, be protected from modification, and be verifiable as correct.[135,141]

Sensitivity label: A hierarchical classification and a set of nonhierarchical components that are used by mandatory access controls to define a process's resource access rights.

Session hijacking: An intruder takes over a connection after the original source has been authenticated.

SET: Secure Electronic Transactions protocol.

SHA: Secure hash algorithm; *see* FIPS PUB 180.[162]

SIGINT: A broad range of operations that involve the interception and analysis of signals across the electromagnetic spectrum.

SIL: Safety integrity level.

Smartcard: A small computer the size of a credit card that is used to perform functions such as identification and authentication.

SML: Strength of mechanism; a rating used by the IA Technical Framework to rate the strength or robustness required for a security mechanism. Currently, three ratings are defined: SML1 — low, SML2 — medium, and SML3 — high. The SML is derived as a function of the value of the information being protected and the perceived threat to it.[152] Compare with SOF.

SMTP: Simple Mail Transfer Protocol.

SNA: Survivable network analysis method; developed by the CERT/CC.

SNMP: Simple Network Management Protocol.

SOF: Strength of function; a rating used by the Common Criteria (ISO/IEC 15408) to rate the strength or robustness required for a security mechanism. Currently, three ratings are defined: basic, medium, and high. The SOF is derived as a function of the value of the information being protected and the perceived threat to it.[120–122] Compare with SML.

Software integrity level: The integrity level of a software item.[58]

Software reliability: A measure of confidence that the software produces accurate and consistent results that are repeatable, under low, normal, and peak loads, in the intended operational environment.[288]

Software reliability case: A systematic means of gathering, organizing, analyzing, and reporting the data needed by internal, contractual, regulatory, and Certification Authorities to confirm that a system has met specified reliability requirements and is fit for use in the intended operational environment; includes assumptions, claims, evidence, and arguments. A software reliability case is a component in a system reliability case.[289]

Software safety: Design features and operational procedures which ensure that a product performs predictably under normal and abnormal conditions, and the likelihood of an unplanned event occurring is minimized and its consequences controlled and contained; thereby preventing accidental injury or death, environmental or property damage, whether intentional or accidental.[288]

Software safety case: A systematic means of gathering, organizing, analyzing, and reporting the data needed by internal, contractual, regulatory and Certification Authorities to confirm that a system has met specified safety requirements and is safe for use in the intended operational environment; includes assumptions, claims, evidence, and arguments. A software safety case is a component in a system safety case.[289]

SPI: Security parameter index; part of IPSec.

Spoofing: Taking on the characteristics of another user, system, or process for the purposes of deception.[362]

SSL3: Secure Socket Layer protocol; *see also* TLS1.

ST: Security target.

Static analysis: Analytical techniques used to assess the safety, reliability, security, and performance of a system without executing it. Static analysis techniques generally fall into seven categories[130]:

1. **Subset analysis** — evaluate whether or not source code complies with the specified safe subset of a language.

2. **Metrics analysis** — evaluate software safety, security, and reliability metrics exhibited by the requirements, design, and source code against the goals specified for these values, such as complexity.
3. **Control flow analysis** — evaluate the structure of the code to determine if the sequence of events is correct under normal and abnormal situations and the presence of sneak circuits, unused, or unreachable code.
4. **Data use analysis** — evaluate whether or not data elements are used as specified.
5. **Information flow analysis** — evaluate that dependencies between inputs and outputs only occur as specified.
6. **Semantic/path analysis** — evaluate the correctness of the translation from formal specification, to design logic, and subsequently code.
7. **Safety, reliability, and security properties analysis** — analyze worst-case conditions for system performance, timing accuracy, capacity loading, etc. against specified safety, reliability, and security requirements.

An advantage of static analysis is that it can be performed throughout the life of a system. Exhibits B.2, B.4, and B.5 (Annex B) cite static analysis techniques.

Steganography: Hiding a message so that it is undetectable by all except those who know of its presence; for example, embedding a message in a document, image, audio, or video recording.

Stream cipher: Encryption algorithms that operate on a single bit or byte of data at a time. Contrast with block ciphers.

Survivability: The capability of a system to fulfill its mission, in a timely manner, in the presence of attacks, failures, or accidents.[336] A survivability assessment covers the full threat control chronology.

System high: A system is operating at system high security mode when the system and all of its local and remote peripherals are protected in accordance with the requirements for the highest classification category and types of material contained in the system. All users having access to the system have a security clearance, but not necessarily a need-to-know for all material contained in the system. In this mode, the design and operation of the system must provide for the control of concurrently available classified material in the system on the basis of need-to-know.[140]

System integrity level: The integrity level of a system.[58]

System reliability: The composite of hardware and software reliability for a specified operational environment. System reliability measurements combine qualitative and quantitative assessments.[337]

System safety: The application of engineering and management principles, criteria, and techniques to achieve acceptable mishap risk, within the constraints of operational effectiveness, time, and cost, throughout the life of a system.[143]

System safety engineering: An engineering discipline that employs specialized professional knowledge and skills in applying scientific and engineering principles, criteria, and techniques to identify and eliminate hazards, in order to reduce the associated mishap risk.[143]

System survivability: The ability to continue to make resources available, despite adverse circumstances including hardware malfunctions, accidental software errors, accidental and malicious intentional user activities, and environmental hazards such as EMC/EMI/RFI.

Systematic failure: Failures that result from an error of omission, error of commission, or operational error during a life-cycle activity.[69]

Systematic safety integrity: A qualitative measure or estimate of the failure rate due to systematic failures in a dangerous mode of failure.[69]

Tampering: An intentionally caused event that results in modification of a system, its intended behavior, or data.[362]

TCB: Trusted computing base.

TCP: Transport Control Protocol.

TCSEC: U.S. Department of Defense Trusted Computer System Evaluation Criteria; *see* CSC-STD-001-83.[135,141]

Telnet: An application layer protocol.

Threat: The potential danger that a vulnerability may be exploited intentionally, triggered accidentally, or otherwise exercised.[362]

Threat analysis: A series of analyses conducted to identify threats and determine their type, source, and severity.

Threat control measure: (1) A proactive design or operational procedure, action, or device used to reduce the risk caused by a threat. (2) A proactive design technique, device, or method designed to eliminate or mitigate hazards, and unsafe and unsecure conditions, modes and states.

Threat perspective: The perspective from which vulnerability/threat analyses are conducted (system owner, administrator, certifier, customer, etc.); also referred to as risk dimension.

Time bomb: A Trojan horse that will trigger when a particular time and/or date is reached.

TLS1: Transport Layer Security protocol.

TNI: Trusted network interpretation of TCSEC; *see* NCSC-TG-011.[145,146]

TOCTTU: Time of check to time of use; the time interval between when a user is authenticated and when they access specific system resources.

TOE: Target of evaluation.

Transport Layer Security protocol: The public version of SSL3, being specified by the IETF.

Transaction path: One of many possible combinations of a series of discrete activities that cause an event to take place. All discrete activities in a transaction path are logically possible. Qualitative or quantitative probability measures can be assigned to a transaction path and its individual activities.

Transport mode: An IPSec protocol used with ESP or Alt in which the ESP or Alt header is inserted between the IP header and the upper-layer protocol of an IP packet.[252]

Trap door: A hidden software or hardware mechanism that permits system protection mechanisms to be circumvented. It is activated in some non-apparent manner; for example, a special "random" key sequence at a terminal.[135,141]

Trojan horse: (1) A program with hidden side effects that are not specified in the program documentation and are not intended by the user executing the program.[277] (2) A computer program with an apparent 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.[135,141]

Trusted computer system: A system that employs sufficient hardware and software integrity measures to allow its use for simultaneously processing a range of sensitive or classified information.

Trusted computing base: The totality of protection mechanisms within a computer system, including hardware, software, and communications equipment, the combination of which is responsible for enforcing a security policy. A TCB consists of one or more components that together enforce a unified security policy over a product or system. The ability of a trusted computing base 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 (such as a user's clearance) related to the security policy.[135,141]

Trusted guard: A computer system that is trusted to enforce a particular guard policy, such as ensuring the flow of only unclassified data from a classified system or ensuring no reverse flow of pest programs from an untrusted system to a trusted system.[362]

Tunnel mode: A IPSec protocol used with ESP in which the header and contents of an IP packet are encrypted and encapsulated prior to transmission, and a new IP header is added.[252]

UDP: User Datagram Protocol.

URL: Uniform resource locator.

Virtual private network: A logical network that connects the geographically dispersed resources of an enterprise over a public network, providing secure global communications across the enterprise without the need for private leased lines.

Virus: An entity that uses the resources of a host computer to reproduce itself and spread, without informed operator action.[416]

VPN: Virtual private network.

Vulnerability: A weakness in a system that can be exploited to violate the system's intended behavior relative to safety, security, reliability, availability, integrity, etc.[362]

Worm: A program that distributes itself in multiple copies within a system or across a distributed system; a worm can be beneficial or harmful.[362]

Worm attack: A harmful exploitation of a worm that can act beyond normally expected behavior, perhaps exploiting security vulnerabilities or causing denials of service.[362]

Wrapper: Encapsulating data or programs to add access controls and monitoring capabilities. Wrappers are used with IPSec and as a confinement technique.