Glossary

Glossary

45 CFR—Code of Federal Regulations Title 45 Public Welfare.

802.11—Family of IEEE standards for wireless LANS first introduced in 1997. The first standard to be implemented, 802.11b, specifies from 1 to 11 Mbps in the unlicensed band using DSSS direct sequence spread spectrum technology. The Wireless Ethernet Compatibility Association (WECA) brands it as Wireless Fidelity (Wi-Fi).

802.1X—An IEEE standard for port based layer two authentications in 802 standard networks. Wireless LANS often use 802.1X for authentication of a user before the user has the ability to access the network.

A/S, A.S., or AS—Under HIPAA, see *administrative simplification.*

AAL—ATM adaptation layer.

AARP—AppleTalk Address Resolution Protocol.

Abduction—A form of inference that generates plausible conclusions (which may not necessarily be true). As an example, knowing that if it is night, then a movie is on television and that a movie is on television, then abductive reasoning allows the inference that it is night.

Abend—Acronym for abnormal end of a task. It generally means a software crash. The abnormal termination of a computer application or job because of a non-system condition or failure that causes a program to halt.

Ability—Capacity, fitness, or tendency to act in specified or desired manner. Skill, especially the physical, mental, or legal power to perform a task.

ABR—Area border router.

Abstraction—The process of identifying the characteristics that distinguish a collection of similar objects; the result of the process of abstraction is a type.

AC—Access Control (Token Ring).

ACC—Audio Communications Controller**.**

Acceptable risk—The level of *residual risk* that has been determined to be a reasonable level of potential loss/disruption for a specific IT system. See also *total risk, residual risk*, and *minimum level of protection*.

Acceptable use policy—A policy that a user must agree to follow to gain access to a network or to the Internet.

Acceptance confidence level—The degree of certainty in a statement of probabilities that a conclusion is correct. In sampling, a specified confidence level is expressed as a percentage of certainty.

Acceptance Inspection—The final inspection to determine whether or not a facility or system meets the specified technical and performance standards. Note: This inspection is held immediately after facility and software testing and is the basis for commissioning or accepting the information system.

Acceptance Testing—The formal testing conducted to determine whether a software system satisfies its acceptance criteria, enabling the customer to determine whether to accept the system.

Access—The ability of a subject to view, change, or communicate with an object. Typically, access involves a flow of information between the subject and the object.

Access Control—The process of allowing only authorized users, programs, or other computer system (i.e., networks) to access the resources of a computer system. A mechanism for limiting use of some resource (system) to authorized users.

Access control certificate—ADI in the form of a security certificate.

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.

Access Control Decision Function (ADF)—A specialized function that makes access control decisions by applying access control policy rules to a requested action, ACI (of initiators, targets, actions, or that retained from prior actions), and the context in which the request is made.

Access Control Decision Information (ADI)—The portion (possibly all) of the ACI made available to the ADF in making a particular access control decision.

Access Control Enforcement Function (AEF)—A specialized function that is part of the access path between an initiator and a target on each access that enforces the decisions made by the ADF.

Access Control Information (ACI)—Any information used for access control purposes, including contextual information.

Access Control List (ACL)—An access control list is the usual means by which access to, and denial of, service is controlled. It is simply a list of the services available, each with a list of the hosts permitted to use the services. Most network security systems operate by allowing selective use of services.

Access Control Mechanisms—Hardware, software, or firmware features and operating and management procedures in various combinations designed to detect and prevent unauthorized access and to permit authorized access to a computer system.

Access control policy—The set of rules that define the conditions under which an access may take place.

Access Controls—The management of permission for logging on to a computer or network.

Access list—A catalog of users, programs, or processes and the specifications of the access categories to which each is assigned.

Access Path—The logical route that an end user takes to access computerized information. Typically, it includes a route through the operating system, telecommunications software, selected application software and the access control system.

Access Period—A segment of time, generally expressed on a daily or weekly basis, during which access rights prevail.

Access protocol—A defined set of procedures that is adopted at an interface at a specified reference point between a user and a network to enable the user to employ the services or facilities of that network.

Access Provider (AP)—Provides a user of some network with access from the user's terminal to that network. This definition applies specifically for the present document. In a particular case, the AP and network operator (NWO) may be a common commercial entity.

Access Rights—Also called permissions or privileges, these are the right granted to users by the administrator or supervisor. These permissions can be read, write, execute, create, delete, etc.

Access Type—The nature of access granted to a particular device, program, or file (e.g., read, write, execute, append, modify, delete, or create).

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. (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.

Accountability—A security principle stating that individuals must be able to be identified. With accountability, violations or attempted violations can be traced to individuals who can be held responsible for their actions.

Accountability—The ability to map a given activity or event back to the responsible party; the property that ensures that the actions of an entity may be traced to that entity.

Accounting—The process of apportioning charges between the home environment, serving network, and user.

Accreditation—A program whereby a laboratory demonstrates that something is operating under accepted standards to ensure quality assurance.

Accreditation—(1) A management or administrative process of accepting a specific site installation/implementation for operational use based upon evaluations and certifications. (2) A formal declaration by a Designated Approving Authority (DAA) that the AIS is approved to operate in a particular security mode using a prescribed set of safeguards. Accreditation is the official management authorization for operation of an AIS and is based on the certification process as well as other management considerations. The accreditation statement affixes security responsibility with the DAA and shows that due care has been taken for security. (3) Formal declaration by a (DAA) that an information system is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk.

Accreditation Authority—Synonymous with Designated Approving Authority (DAA).

Accreditation boundary—All components of an information system to be accredited by designated approving authority and excluding separately accredited systems, to which the information system is connected. .

Accreditation letter—The accreditation letter documents the decision of the authorizing official and the rationale for the accreditation decision and is documented in the final accreditation package, which consists of the accreditation letter and supporting documentation. .

Accreditation Package—A product of the certification effort and the main basis for the accreditation decision. Note: The accreditation package, at a minimum, will include a recommendation for the accreditation decision and a statement of residual risk in operating the system in its environment. Other information included may vary depending on the system and the DAA.

Accredited—Formally confirmed by an accreditation body as meeting a predetermined standard of impartiality and general technical, methodological, and procedural competence.

Accredited Standards Committee (ASC)— An organization that has been accredited by ANSI for the development of American National Standards.

Accrediting Authority—Synonymous with Designated Approving Authority (DAA).

Accumulator—An area of storage in memory used to develop totals of units or items being computed.

Accuracy—A performance criterion that describes the degree of correctness with which a function is performed.

ACF—User data protection access control functions.

ACG—Ambulatory Care Group.

ACH—See Automated Clearinghouse.

ACI—Access control information.

ACK—Acknowledgment.

Acknowledgment (ACK)—A type of message sent to indicate that a block of data arrived at its destination without error. A negative acknowledgment is called a “NAK.”.

ACL—See *access control list.*

ACM—Configuration management assurance class.

Acquisition Organization—The government organization that is responsible for developing a system.

Acquisition, development, and installation controls—The process of assuring that adequate controls are considered, evaluated, selected, designed, and built into the system during its early planning and development stages and that an on-going process is established to ensure continued operation at an acceptable level of risk during the installation, implementation, and operation stages.

ACR—Abbreviation for Acoustic Conference Room, an enclosure which provides acoustic but not electromagnetic emanations shielding; ACRs are no longer procured; TCRs are systematically replacing them.

Acrostic—A poem or series of lines in which certain letters, usually the first in each line, form a name, motto, or message when read in sequence.

Action—The operations and operands that form part of an attempted access.

Action ADI—Action decision information associated with the action.

Active Object—An object that has its own process; the process must be ongoing while the active object exists.

Active System—A system connected directly to one or more other systems. Active systems are physically connected and have a logical relationship to other systems.

Active threat—The threat of a deliberate unauthorized change to the state of the system.

Active Wiretapping—The attachment of an unauthorized device (e.g., a computer terminal) to a communications circuit to gain access to data by generating false messages or control signals or by altering the communications of legitimate users.

ActiveX—Microsoft's Windows-specific non-Java technique for writing applets. ActiveX applets take considerably longer to download than the equivalent Java applets; however, they more fully exploit the features of Windows. .

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

Ad blocker—Software placed on a user's personal computer that prevents advertisements from being displayed on the Web. Benefits of an ad blocker include the ability of Web pages to load faster and the prevention of user tracking by ad networks. .

Ada—A programming language that allows use of structured techniques for program design; concise but powerful language designed to fill government requirements for real-time applications.

Adaptive Array (AA)—Continually monitors received signal for interference. The antenna automatically adjusts its directional characteristics to reduce the interference. Also called adaptive antenna array.

Adaptive filter—Prompts user to rate products or situations and also monitors your actions over time to find out what you like and dislike.

Adaptivity—The ability of intelligent agents to discover, learn, and take action independently.

Add-On Security—The retrofitting of protection mechanisms, implemented by hardware, firmware, or software, on a computer system that has become operational.

Address—(1) A sequence of bits or characters that identifies the destination and sometimes the source of a transmission. (2) An identification (e.g., number, name, or label) for a location in which data is stored.

Address mapping—The process by which an alphabetic Internet address is converted into a numeric IP address, and vice versa.

Address Mask—A bit mask used to identify which bits in an IP address correspond to the network address and subnet portions of the address. This mask is often referred to as the subnet mask because the network portion of the address can be determined by the class inherent in an IP address. The address mask has ones in positions corresponding to the network and subnet numbers and zeros in the host number positions.

Address Resolution—A means for mapping network layer addresses onto media-specific addresses.

Address Resolution Protocol (ARP)—The Internet protocol used to dynamically map Internet addresses to physical (hardware) addresses on the local area network. Limited to networks that support hardware broadcast.

Adequate security—Security commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information. This includes assuring that systems and applications operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost-effective management, acquisition, development, installation, operational, and technical controls.

ADG— Ambulatory Diagnostic Group.

Adjacent channel interference—Interference of a signal caused by signal transmissions of another frequency too close in proximity.

ADM—Guidance documents, administrator guidance.

Administrative Code Sets— Code sets that characterize a general business situation, rather than a medical condition or service. Under HIPAA, these are sometimes referred to as nonclinical or nonmedical code sets. Compare to medical code sets.

Administrative Controls—The actions or controls dealing with operational effectiveness, efficiency and adherence to regulations and management policies.

Administrative security—The management constraints, operational procedures, accountability procedures, and supplemental controls established to provide an acceptable level of protection for sensitive data.

Administrative security information—Persistent information associated with entities; it is conceptually stored in the Security Management Information Base. Examples are: security attributes associated with users and set up on user account installation, which is used to configure the user's identity and privileges within the system information configuring a secure interaction policy between one entity and another entity, which is used as the basis for the establishment of operational associations between those two entities.

Administrative Services Only (ASO)—An arrangement whereby a self-insured entity contracts with a Third-Party Administrator (TPA) to administer a health plan.

Administrative Simplification (A/S)—Title II, Subtitle F of HIPAA, which gives HHS the authority to mandate the use of standards for the electronic exchange of healthcare data; to specify what medical and administrative code sets should be used within those standards; to require the use of national identification systems for healthcare patients, providers, payers (or plans), and employers (or sponsors); and to specify the types of measures required to protect the security and privacy of personally identifiable healthcare information. This is also the name of Title II, Subtitle F, Part C of HIPAA.

ADO—Delivery and operation assurance class.

ADSL—Asymmetric Digital Subscriber Line.

ADSP—AppleTalk Data Stream Protocol.

ADV—Development assurance class.

Adversary—Any individual, group, organization, or government that conducts activities, or has the intention and capability to conduct activities, detrimental to critical assets.

Advisory Sensitivity Attributes—User-supplied indicators of file sensitivity that alert other users to the sensitivity of a file so that they may handle it appropriate to its defined sensitivity. Advisory sensitivity attributes are not used by the AIS to enforce file access controls in an automated manner.

Adware—Software to generate ads that installs itself on your computer when you download some other (usually free) program from the Web.

AEF—Access control enforcement function.

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.

AFEHCT—See the Association for Electronic Health Care Transactions.

Affiliate programs—Arrangements made between E-commerce sites that direct users from one site to the other and by which, if a sale is made as a result, the originating site receives a commission.

Affordability—Extent to which C4I features are cost effective on both a recurring and nonrecurring basis.

AFL—Authentication failures.

AFP—AppleTalk File Protocol.

AGD—Guidance documents assurance class.

Agent—In the client/server model, the part of the system that performs information preparation and exchange on behalf of a client or server application.

Aggregate information—Information that may be collected by a Web site but is not "personally identifiable" to you. Aggregate information includes demographic data, domain names, Internet provider addresses, and Web site traffic. As long as none of these fields is linked to a user's personal information, the data is considered aggregate. .

Aggregation—A relation, such as CONSISTS OF or CONTAINS, between types that defines the composition of a type from other types.

Aging—The identification, by date, of unprocessed or retained items in a file. This is usually done by date of transaction, classifying items according to ranges of data.

AH—Authentication Header.

Alarm collector function—A function that collects the security alarm messages, translates them into security alarm records, and writes them to the security alarm log.

Alarm examiner function—A function that interfaces with a security alarm administrator.

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.

ALC—Lifecycle support assurance class.

ALE—Annual loss expectancy.

Algorithm—A computing procedure designed to perform a task such as encryption, compression, or hashing.

Aliases—Used to reroute browser requests from one URL to another.

Alphabetic test—The check on whether an element of data contains only alphabetic or blank characters.

Alphanumeric—A character set that includes numeric digits, alphabetic characters, and other special symbols.

Alternate Mark Inversion (AMI)—The line coding format in T-1 transmission systems whereby successive 1s (marks) are alternately inverted (sent with polarity opposite that of the preceding mark).

Alternating Current (AC)—Typically, the 120-V electricity delivered by the local power utility to the three-pin power outlet in the wall. The polarity of the current alternates between plus and minus, 60 times per second.

AM—Amplitude modulation.

Ambulatory Payment Class (APC)— A payment type for outpatient PPS claims.

Amendment— See Amendments and Corrections.

Amendments and Corrections— In the final privacy rule WHAT PRIVACY RULE?, an amendment to a record would indicate that the data is in dispute while retaining the original information, whereas a correction to a record would alter or replace the original record.

American National Standards (ANS)— Standards developed and approved by organizations accredited by ANSI.

American National Standards Institute (ANSI)—The agency that recommends standards for computer hardware, software, and firmware design and use.

American Registry for Internet Numbers (ARIN)—A nonprofit organization established for the purpose of administration and registration of Internet Protocol (IP) numbers to the geographical areas currently managed by Network Solutions (InterNIC). Those areas include, but are not limited to North America, South America, South Africa, and the Caribbean.

American Society for Testing and Materials (ASTM)—A standards group that has published general guidelines for the development of standards, including those for healthcare identifiers. ASTM Committee E31 on Healthcare Informatics develops standards on information used within healthcare.

American Standard Code for Information Interchange (ASCII)—A byte-oriented coding system based on an 8-bit code and used primarily to format information for transfer in a data communications environment.

AMI—Alternate Mark Inversion (T1/E1).

AMIA— See the American Medical Informatics Association.

Ampere (amp)—A unit of measurement for electric current. One volt of potential across a 1-ohm impedance causes a current flow of 1 ampere.

Amplitude Modulation (AM)—The technique of varying the amplitude or wavelength of a carrier wave in direct proportion to the strength of the input signal while maintaining a constant frequency and phase.

AMT—Protection of the TSF, underlying abstract machine test.

Analog—A voice transmission mode that is not digital in which information is transmitted in its original form by converting it to a continuously variable electrical signal.

Analysis and Design Phase—The phase of the systems development life cycle in which an existing system is studied in detail and its functional specifications are generated.

Anamorphosis—An image or the production of an image that appears distorted unless it is viewed from a special angle or with a special instrument.

Annual Loss Expectancy (ALE)—In risk assessment, the average monetary value of losses per year.

ANO—Privacy, anonymity.

Anonymity—The state in which something is unknown or unacknowledged.

Anonymizer—A service that prevents Web sites from seeing a user's Internet Protocol (IP) address. The service operates as an intermediary to protect the user's identity. .

Anonymous File Transfer Protocol (FTP)—A method for downloading public files using the File Transfer Protocol. Anonymous FTP is called anonymous because users do not provide credentials before accessing files from a particular server. In general, users enter the word anonymous when the host prompts for a username; anything can be entered for the password, such as the user's email address or simply the word guest. In many cases, an anonymous FTP site will not even prompt for a name and password.

Anonymous Web Browsing (AWB)—Services hide your identity from the Web sites you visit.

ANS— See American National Standards.

ANSI—*See* American National Standards Institute.

Antenna gain—The measure in decibels of how much more power an antenna will radiate in a certain direction with respect to that which would be radiated by a reference antenna.

Anti-Air Warfare (AAW)—A primary warfare mission area dealing with air superiority.

Anti-Submarine Warfare (ASW)—A primary warfare mission area aimed against the subsurface threat.

Anti-Surface Warfare (ASUW)—A primary warfare mission area dealing with sea-going, surface platforms.

Anti-virus Software—Applications that detect prevent and possibly remove all known viruses from files located in a microcomputer hard drive.

APC— See Ambulatory Payment Class.

APE—Protection profile evaluation assurance class.

API—Application Programming Interface. The interface between the application software and the application platform, across which all services are provided. The application programming interface is primarily in support of application portability, but system and application interoperability are also supported by a communication API.

Applet—A small Java program embedded in an HTML document.

Application—Computer software used to perform a distinct function. Also used to describe the function itself.

Application architects—IT professionals who can design creative technology-based business solutions.

Application Controls—The transaction and data relating to each computer-based application system. Therefore, they are specific to each such application controls, which may be manual or programmed, are to endure the completeness and accuracy of the records and the validity of the entries made therein resulting from both manual and programmed processing. Examples of application controls include data input validation, agreement of batch controls and encryption of data transmitted.

Application generation subsystem—Contains facilities to help you develop transaction-intensive applications.

Application layer—The top-most layer in the OSI Reference Model providing such communication service is invoked through a software package. This layer provides the interface between end-users and networks. It allows use of e-mail and viewing Web pages, along with numerous other networking services.

Application Objects—Applications and their components that are managed within an object-oriented system. Example operations on such objects are OPEN, INSTALL, MOVE, and REMOVE.

Application Program Interface (API)—A set of calling conventions defining how a service is invoked through a software package.

Application programs—Computer software designed for a specific job, such as word processing, accounting, spreadsheet, etc.

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.

Application Service Provider (ASP)—Provides an outsourcing service for business software applications.

Application software—Software that enables you to solve specific problems or perform specific tasks.

APPN—Advanced peer-to-peer networking.

Approval to operate—See *certification* and *accreditation.*

Architecture—The structure or ordering of components in a computational or other system. The classes and the interrelation of the classes define the architecture of a particular application. At another level, the architecture of a system is determined by the arrangement of the hardware and software components. The terms "logical architecture" and "physical architecture" are often used to emphasize this distinction.

ARCNET—Developed by Datapoint Corporation in the 1970s; a LAN (Local Area Network) technology that competed strongly with Ethernet, but no longer does. Initially a computer connected via ARCNET could communicate at 2.5 Mbps, although this technology now supports a throughput of 20 Mbps (compared to current Ethernet at 100 Mbps and 1 Gbps).

Arithmetic Logic Unit (ALU)—A component of the computer's processing unit, in which arithmetic and matching operations are performed.

Arithmetic operator—In programming activities, a symbol representing an arithmetic calculation or process.

ARP—Address Resolution Protocol. This is a protocol that resides in the TCP/IP suite of protocols. Its purpose is to associate IP addresses at the network layer with MAC addresses at the data link layer.

ARPA—Advanced Research Projects Agency.

Array—Consecutive storage areas in memory that are identified by the same name. The elements (or groups) within these storage areas are accessed through subscripts.

Artificial Intelligence (Al)—A field of study involving techniques and methods under which computers can simulate such human intellectual activities as learning.

Artificial Neural Network (ANN)—Also called a neural network; an artificial intelligence system that is capable of finding and differentiating patterns.

AS—Authentication server; part of Kerberos KDC.

ASBR—Autonomous system boundary router.

ASC— See Accredited Standards Committee.

ASCII—American Standard Code for Information Interchange.

ASE—Security Target evaluation assurance class.

ASIC—Application-specific integrated circuit.

ASIS—American Society Industrial Security.

ASK—Amplitude shift keying.

ASO— See Administrative Services Only.

ASP—AppleTalk Session Protocol.

ASP/MSP—A third party provider that delivers and manages applications and computer services, including security services to multiple users via the Internet or Virtual Private Network (VPN).

ASPIRE— AFEHCT's Administrative Simplification Print Image Research Effort work group.

Assembler Language—A computer programming language in which alphanumeric symbols represent computer operations and memory addresses. Each assembler instruction translates into a single machine language instruction.

Assembler Program—A program language translator that converts assembler language into machine code.

Assertion—Explicit statement in a system security policy that security measures in one security domain constitute an adequate basis for security measures (or lack of them) in another.

Assessment—(1) An effort to gain insight into system capabilities and limitations. May be conducted in many ways including a paper analysis, laboratory type testing, or even through limited testing with operationally representative users and equipment in an operational environment. Not sufficiently rigorous in and of itself to allow a determination of effectiveness and suitability to be made for purposes of operational testing. (2) Surveys and Inspections; an analysis of the vulnerabilities of an AIS. Information acquisition and review process designed to assist a customer to determine how best to use resources to protect information in systems.

Asset—Any person, facility, material, information, or activity which has a positive value to an owner.

Association Control Service Element (ACSE)—Part of the application layer of the OSI Model. ASCE provides the means to exchange authentication information coming from the Specific Application Service Element (SASE) of the OSI Model.

Association for Electronic Health Care Transactions (AFEHCT)— An organization that promotes the use of EDI in the healthcare industry.

Association-security-state—The collection of information that is relevant to the control of communications security for a particular application-association.

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.

Assurance—(1) Grounds for confidence that the other four security goals (integrity, availability, confidentiality, and accountability) have been adequately met by a specific implementation. “Adequately met” includes the following: functionality that performs correctly, sufficient protection against unintentional errors (by users or software), and sufficient resistance to malicious penetration or by-pass. (2) A measure of confidence that the security features and architecture of an AIS accurately mediate and enforce the security policy. (3) A measure of confidence that the security features and architecture of an AIS accurately mediate and enforce the security policy. Note: Assurance refers to a basis for believing that the objective and approach of a security mechanism or service will be achieved. Assurance is generally based on factors such as analysis involving theory, testing, software engineering, validation, and verification. Life-cycle assurance requirements provide a framework for secure system design, implementation, and maintenance. The level of assurance that a development team, certifier, or accreditor has about a system reflects the confidence that they have that the system will be able to enforce its security policy correctly during use and in the face of attacks. Assurance may be provided through four means: 1. the way the system is designed and built, 2. analysis of the system description for conformance to requirement and for vulnerabilities, 2. testing the system itself to determine its operating characteristics, and 4. operational experience. Assurance is also provided through complete documentation of the design, analysis, and testing.

ASTM— See the American Society for Testing and Materials.

Asymmetric cryptosystem—This is an information system utilizing an algorithm or series of algorithms which provide a cryptographic key pair consisting of a private key and a corresponding public key. The keys of the pair have the properties that (1) the public key can verify a digital signature that the private key creates, and (2) it is computationally infeasible to discover or derive the private key from the public key. The public key can therefore be disclosed without significantly risking disclosure of the private key. This can be used for confidentiality as well as for authentication.

Asymmetric Key (Public Key)—A cipher technique whereby different cryptographic keys are used to encrypt and decrypt a message.

Asynchronous—A variable or random time interval between successive characters, blocks, operations, or events. Asynchronous data transmission provides variable intercharacter time but fixed interbit time within characters.

Asynchronous Transfer Mode—ATM is a high-bandwidth, low-delay switching and multiplexing technology. It is a data-link layer protocol. This means that it is a protocol-independent transport mechanism. ATM allows very high-speed data transfer rates at up to 155 Mbps. Data is transmitted in the form of 53-byte units called cells. Each cell consists of a 5-byte header and a 48-byte payload. The term “asynchronous” in this context refers to the fact that cells from any one particular source need not be periodically spaced within the overall cell stream. That is, users are not assigned a set position in a recurring frame as is common in circuit switching. ATM can transport audio/video/data over the same connection at the same time and provide QoS (Quality of Service) for this transport.

ATD—Identification and authentication user attribute definition.

ATE—Tests assurance class.

ATM—See Asynchronous Transfer Mode. .

Atomicity—The assurance that an operation either changes the state of all participating objects consistent with the semantics of the operation or changes none at all.

Atoms—The smallest particle of an element that can exist alone or in combination.

ATP—AppleTalk Transaction Protocol.

Attenuation—The decrease in power of a signal, light beam, or light wave, either absolutely or as a fraction of a reference value. The decrease usually occurs as a result of absorption, reflection, diffusion, scattering, deflection, or dispersion from an original level and usually not as a result of geometric spreading.

Attribute—A characteristic defined for a class. Attributes are used to maintain the state of the object of a class. Values can be connected to objects via the attributes of the class. Typically, the connected value is determined by an operation with a single parameter identifying the object. Attributes implement the properties of a type.

Audio masking—a condition where one sound interferes with the perception another sound.

Audio output—Voice synthesizers that create audible signals resembling a human voice out of computer-generated output.

Audio response system—The method of delivering output by using audible signals and transmitters that simulate a spoken language.

Audit—An independent review and examination of system records and activities that test for the adequacy of system controls, ensure compliance with established policy and operational procedures, and recommend any indicated changes in controls, policy, and procedures.

Audit authority—The manager responsible for defining those aspects of a security policy applicable to maintaining a security audit.

Audit event detector function—A function that detects the occurrence of security-relevant events. This function is normally an inherent part of the functionality implementing the event.

Audit recorder function—A function that records the security-relevant messages in a security audit trail.

Audit Review—The independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies or procedures.

Audit risk—The probable unfavorable monetary effect related to the occurrence of an undesirable event or condition.

Audit trail—A chronological record of system activities that is sufficient to enable the reconstruction, review, and examination of each event in a transaction from inception to output of final results.

Audit trail analyzer function—A function that checks a security audit trail in order to produce, if appropriate, security alarm messages.

Audit trail archiver function—A function that archives a part of the security audit trail.

Audit trail collector function—A function that collects individual audit trail records into a security audit trail.

Audit trail examiner function—A function that builds security reports out of one or more security audit trails.

Audit trail provider function—A function that provides security audit trails according to some criteria.

Audit Trail/Log—Application or system programs when activated automatically monitor system activity in terms of on-line users, accessed programs, periods of operation, file accesses, etc.

AUI—Attachment unit interface.

AURP—AppleTalk Update-Based Routing Protocol.

AUT—CM automation.

Authenticate—To verify the identity of a user, user device, or other entity, or the integrity of data stored, transmitted, or otherwise exposed to possible unauthorized modification in an automated information system, or establish the validity of a transmitted message.

Authenticated identity—An identity of a principal that has been assured through authentication.

Authentication—The act of identifying or verifying the eligibility of a station, originator, or individual to access specific categories of information. Typically, a measure designed to protect against fraudulent transmissions by establishing the validity of a transmission, message, station, or originator.

Authentication certificate—Authentication information in the form of a security certificate which may be used to assure the identity of an entity guaranteed by an authentication authority.

Authentication exchange—A sequence of one or more transfers of exchange authentication information (AI) for the purposes of performing an authentication.

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

Authentication Information (AI)—Information used to establish the validity of a claimed identity.

Authentication initiator—The entity which starts an authentication exchange.

Authentication method—Method for demonstrating knowledge of a secret. The quality of the authentication method, its strength is determined by the cryptographic basis of the key Architecture for Public-Key Infrastructure (APKI) Draft distribution service on which it is based. A symmetric key based method, in which both entities share common authentication information, is considered to be a weaker method than an asymmetric key based method, in which not all the authentication information is shared by both entities.

Authenticity—(1) The ability to ensure that the information originates or is endorsed from the source which is attributed to that information. (2) The service that ensures that system events are initiated by and traceable to authorized entities. It is composed of authentication and nonrepudiation.

Authorization—The granting of right of access to a user, program, or process.

Authorization policy—A set of rules, part of an access control policy, by which access by security subjects to security objects is granted or denied. An authorization policy may be defined in terms of access control lists, capabilities or attributes assigned to security subjects, security objects or both.

Authorize processing—See accreditation.

Authorized Access List—A list developed and maintained by the information systems security officer of personnel who are authorized unescorted access to the computer room.

Authorizing official—Official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals. .

Autofilter function—Filters a list and allows you to hide all the rows in a list except those that match criteria you specify.

Automated Clearinghouse (ACH)— See Health Care Clearinghouse.

Automated Information System (AIS)— (1) An assembly of computer hardware, software, firmware, and related peripherals configured to collect, create, compute, disseminate, process, store, and control data or information; and (2) Information systems that manipulate, store, transmit, or receive information, and associated peripherals such as input/output and data storage and retrieval devices and media.

Automated information system security program—synonymous with *Information technology security program.*

Automated security monitoring—The use of automated procedures to ensure that the security controls implemented within a computer system or network are not circumvented or violated.

Automatic Call Distribution (ACD)—A specialized phone system originally designed simply to route incoming calls to all available personnel so that calls are evenly distributed. An ACD recognizes and answers an incoming call, looks in its database for instructions on what to do with that call, sends the call to a recording or voice response unit or to an available operator.

Automatic Speech Recognition (ASR)—A system that not only captures spoken words but also distinguishes word groupings to form sentences.

Autonomy—The ability of an intelligent agent to act without your telling it every step to take.

AVA—Vulnerability assessment assurance class.

Availability—The property of being accessible and usable upon demand by an authorized entity.

Availability formula—This formula is used to calculate how reliable the equipment that is being installed will be for a particular application.

Awareness—Awareness programs set the stage for training by changing organizational attitudes toward realization of the importance of security and the adverse consequences of its failure. [NIST SP 800-18].

Awareness, training, and education controls—Awareness programs that set the stage for training by changing organizational attitudes to realize the importance of security and the adverse consequences of its failure; training that teaches people the skills that will enable them to perform their jobs more effectively; and education that is targeted for IT security professionals and focuses on developing the ability and vision to perform complex, multidisciplinary activities.

B2B marketplace—An internet-based service that brings together many buyers and sellers.

Backbone—The primary connectivity mechanism of a hierarchical distributed system. All systems that have connectivity to an intermediate system on the backbone are assured of connectivity to each other.

Backbone network—A network that interconnects various computer networks and mainframe computers in an enterprise. The backbone provides the structure through which computers communicate.

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. (See also trap door.).

Backoff—The (usually random) retransmission delay enforced by contentious MAC protocols after a network node with data to transmit determines that the physical medium is already in use.

Back-propagation neural network—A neural network trained by someone.

Backup and Recovery—The ability to recreate current master files using appropriate prior master records and transactions.

Backup operation—A method of operation used to complete essential tasks (as identified by risk analysis) subsequent to the disruption of the information processing facility and continuing to do so until the facility is sufficiently restored.

Backup Procedures—Provisions make for the recovery of data files and program libraries and for the restart or replacement of computer equipment after the occurrence of a system failure or disaster.

Backward chaining—A process related to an expert system inference engine that starts with a hypothesis and attempts to confirm that the hypothesis is consistent with information in the knowledge base.

Bandwidth—Difference between the highest and lowest frequencies available for network signals. The term is also used to describe the rated throughput capacity of a given network medium or protocol.

Banner ad—A small ad on one Web site that advertises the products and services of another business.

Bar code—A series of solid bars of different widths used to encode data. Special optical character recognition (OCR) devices can read this data.

Bar code reader—Captures information that exists in the form of vertical bars whose width and distance from each other determine a number.

Baseband—A form of modulation in which data signals are pulsed directly on the transmission medium without frequency division and usually utilize a transceiver. In baseband the entire bandwidth of the transmission medium (cable) is utilized for a single channel. It uses a single carrier frequency and requires all stations attached to the network to participate in every transmission. *See* broadband.

Baseline—[NCSC029, 1994]: A set of critical observations or data used for a comparison or control. Note: Examples include a baseline security policy, a baseline set of security requirements, and a baseline system.

Baseline Architecture—[SPAWAR, 1987b]: A complete list and description of equipment that can be found in operation today.

Baseline security—the minimum security controls required for safeguarding an IT system based on its identified needs for confidentiality, integrity, and availability protection.

BASIC—See Beginner’s All-Purpose Symbolic Instruction Code.

Basic Rate Interface (BRI)—Supports a total signaling rate of 144 kbps, which is divided into two B or bearer channels running at 64 kbps, and a D or data channel runing at 16 kbps. The bearer channels carry the actual voice, video, or data information and the D channel is used for signaling.

Basic Service Set (BSS)—Basic Service Set is a set of 802.11-compliant stations that operate as a fully connected wireless network.

Basic text formatting tag—HTML tags that allow you to specify formatting for text.

Batch control—A computer information processing technique in which numeric fields are totaled and records are tabulated to provide a comparison check for subsequent processing results.

Baud—Signal or state change during data transmission. Each state change can be equal to multiple bits, so the actual bit rate during data transmission may exceed the baud rate.

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.

BBA— The Balanced Budget Act of 1997.

BBN—Bayesian Belief network.

BBRA— The Balanced Budget Refinement Act of 1999.

BBS—*see* Bulletin Board System.

BCBSA— See Blue Cross and Blue Shield Association.

BCP—The newest subseries of RFCs that are written to describe Best Current Practices in the Internet. Rather than specify the best ways to use the protocols and the best ways to configure options to ensure interoperability between various vendors' products, BCPs carry the endorsement of the IESG.

BDR—Backup designated router.

Beamwidth—The width of the main lobe of an antenna pattern, usually defined as 3 db down from the peak of the lobe.

BECN—Backward Explicit Congestion Notification (Frame Relay).

Beginner's All-Purpose Symbolic Instruction Code (BASIC)—A programming language designed in the 1960s to teach students how to program and to facilitate learning. The powerful language syntax was designed especially for time-sharing systems.

Behavioral outcome—what an individual who has completed the specific training module is expected to be able to accomplish in terms of IT security-related job performance.

Behaviorally Object-Oriented—[Manola, 1990]: The data model incorporates features to define arbitrarily complex object types together with a set of specific operators (abstract data types).

Benchmark test—A simulation evaluation conducted before purchasing or leasing equipment to determine how well hardware, software, and firmware perform.

Benign Environment—[NCSC004, 1988]: A nonhostile environment that may be protected from external hostile elements by physical, personnel, and procedural security countermeasures.

Benign System—[DoD8510, 2000]: A system that is not related to any other system. Benign systems are closed communities without physical connection or logical relationship to any other system. Benign systems are operated exclusive of one another and do not share users, information, or end processing with other systems.

BER—Bit error rate.

Bespoke learning materials—Materials that are designed and tailored to meet an organization's specific learning needs and outcomes. British Learning Association Glossary: http://www.baol.co.uk/glossary.htm.

Best-effort QoS—The lowest of all QoS traffic classes. If the guaranteed QoS cannot be delivered, the bearer network delivers the QoS, which is called best-effort QoS.

Best-effort service—A service model that provides minimal performance guarantees, allowing an unspecified variance in the measured performance criteria.

Between-the-Lines Entry—Access obtained through the use of active wiretapping by an unauthorized user to a momentarily inactive terminal of a legitimate user assigned to a communications channel.

BGP—Border Gateway Protocol.

BIA (1)—Business impact analysis.

BIA (2)—Burned-in address.

Billing—A function whereby CDRs generated by the charging function are transformed into bills requiring payment.

Binary—Where only two values or states are possible for a particular condition, such as "on" or "off" or "1" or "0." Binary is the way digital computers function because it represents data as on or off.

Binary digit—A state of function represented by the digit 0 or 1.

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

Biometrics—A security technique that verifies an individual's identity by analyzing a unique physical attribute, such as a handprint.

BIOS—The BIOS is built-in software that determines what a computer can do without accessing programs from a disk. On PCs, the BIOS contains all the code required to control the keyboard, display screen, disk drives, serial communications, and a number of miscellaneous functions.

Bipolar 8 zero substitution (B8ZS)—A technique used to accommodate the density requirement for digital T-carrier facilities in the public network, while allowing 64 kbps clear data per channel.

Rather than inserting a 1 for every seven consecutive 0s, B8ZS inserts two violations of bipolar line encoding technique for digital transmission links.

B-ISDN—Broadband ISDN.

Bit—A binary value represented by an electronic component that has a value of 0 or 1.

BIT—Built-in test.

Bit Error Rate (BER)—The probability that a particular bit will have the wrong value.

Bit Map—A specialized form of an index indicating the existence or nonexistence of a condition for a group of blocks or records. Although they are expensive to build and maintain, they provide very fast comparison and access facilities.

Bit Mask—A pattern of binary values that is combined with some value using bitwise AND with the result that bits in the value in positions where the mask is zero are also set to zero.

Bit Rate—This is the speed at which bits are transmitted on a circuit, usually expressed in bits per second.

Bits Per Second (BPS)—The speed at which bits are sent during data transmission.

Bit-stream Image—Bit-streams backups (also referred to as mirror image backups) involve all areas of a computer hard disk drive or another type of storage media. Such backups exactly replicate all sectors on a given storage device. Thus, all files and ambient data storage areas are copied.

Black—[12 FAM 090]: In the information processing context, black denotes data, text, equipment, processes, systems or installations associated with unencrypted information that requires no emanations security related protection. For example, electronic signals are "black" if bearing unclassified information. Antonym: Red. [NSTISSI 4009]: Designation applied to information systems, and to associated areas, circuits, components, and equipment, in which national security information is not processed.

Black-hat hackers—Cyber vandals.

Blind scheme—an extraction process method that can recover the hidden message by means only of the encoded data.

Block Cipher—A method of encrypting text to produce ciphertext in which a cryptographic key and algorithm are applied to a block of data as a group instead of one bit at a time.

Block structure—In programming, a segment of code that can be treated as an independent module.

Blocking factor—The number of records appearing between interblock gaps on magnetic storage media.

Blog—(1) A contraction of weblog, a form of online writing characterized in format by a single column of chronological text, usually with a sidebar, and frequently updated. As of mid-2002, the vast majority of blogs are nonprofessional (with only a few experimental exceptions) and are run by a single writer. (2) To write an article on a blog. Samizdata.net: http://www.samizdata.net/blog/glossary.html.

BLP—Bypass Label Processing.

Blue Cross and Blue Shield Association (BCBSA)— An association that represents the common interests of Blue Cross and Blue Shield health plans. The BCBSA serves as the administrator for the Health Care Code Maintenance Committee and also helps maintain the HCPCS Level II codes.

Bluetooth—Technology that provides entirely wireless connections for all kinds of communication devices.

Body—One of four possible components of a message. Other components are the headings, attachment, and the envelope.

Bootleg—an unauthorized recording of a live or broadcast performance. They are duplicated and sold without the permission of the artist, composer or record company.

BOOTP—Bootstrap Protocol.

Bote-swaine cipher—a steganographic cipher used by Francis Bacon to insert his name within the text of his writings.

Bounds Checking—The testing of computer program results for access to storage outside of its authorized limits.

Bounds register—A hardware or firmware register that holds an address specifying a storage boundary.

Boyd Cycle—[JITC, 1999]: See OODA Loop and J. Boyd, Patterns of Conflict, December 1986. Unpublished study, 196 pages [Boyd, 1986].

BP— See Business Partner.

BPDU—Bridge Protocol Data Unit.

Bps—Bits per second.

Branch—An alteration of the normal sequential execution of program statements.

Brevity lists—A coding system that reduces the time required to transmit information by representing long, stereotyped sentences with only a few characters.

BRI—Basic rate interface (ISDN).

Bridge—A device that connects two or more physical networks and forwards packets between them. Bridges can usually be made to filter packets, that is, to forward only certain traffic.

Broadband—Characteristic of any network that multiplexes multiple, independent network carriers onto a single cable. Broadband technology allows several networks to coexist on one single cable; traffic from one network does not interfere with traffic from another because the conversations happen on different frequencies in the "ether," rather like the commercial radio system.

Broadcast—A packet delivery system where a copy of a given packet is given to all hosts attached to the network. Example: Ethernet.

Broadcast Storm—A condition that can occur on broadcast type networks such as Ethernet. This can happen for a number of reasons, ranging from hardware malfunction to configuration error and bandwidth saturation.

Brouter—A concatenation of "bridge" and "router." Used to refer to devices that perform both bridging and routing.

Browser—Short for *Web browser,* a software application used to locate and display Web pages. The two most popular browsers are Netscape Navigator and Microsoft Internet Explorer. Both of these are *graphical browsers,* which means that they can display graphics as well as text. In addition, most modern browsers can present multimedia information, including sound and video, although they require plug-ins for some formats.

Browser-safe colors—A range of 216 colors that can be represented using 8 bits and are visible in all browsers.

Browsing—The searching of computer storage to locate or acquire information, without necessarily knowing whether it exists or in what format.

Brute Force—The name given to a class of algorithms that repeatedly try all possible combinations until a solution is found.

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.

Buffer *(n)*—A temporary storage area, usually in RAM. The purpose of most buffers is to act as a holding area, enabling the CPU to manipulate data before transferring it to a device. Because the processes of reading and writing data to a disk are relatively slow, many programs keep track of data changes in a buffer and then copy the buffer to a disk. For example, word processors employ a buffer to keep track of changes to files. Then when you *save* the file, the word processor updates the disk file with the contents of the buffer. This is much more efficient than accessing the file on the disk each time you make a change to the file. Note that because your changes are initially stored in a buffer, not on the disk, all of them will be lost if the computer fails during an editing session. For this reason, it is a good idea to save your file periodically. Most word processors automatically save files at regular intervals. Another common use of buffers is for printing documents. When you enter a PRINT command, the operating system copies your document to a print buffer (a free area in memory or on a disk) from which the printer can draw characters at its own pace. This frees the computer to perform other tasks while the printer is running in the background. Print buffering is called *spooling* . Most keyboard drivers also contain a buffer so that you can edit typing mistakes before sending your command to a program. Many operating systems, including DOS, also use a *disk buffer* to temporarily hold data that they have read from a disk. The disk buffer is really a cache.

Bug—A coded program statement containing a logical or syntactical error.

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.

Bulletin Board System (BBS)—A computer that allows you to log on and post messages to other subscribers to the service. To use a BBS, a modem and the telephone number of the BBS is required. A BBS application runs on a computer and allows people to connect to that computer for the purpose of exchanging e-mail, chatting, and file transfers. A BBS is not part of the Internet.

Burn Box—A device used to destroy computer data. Usually a box with magnets or electrical current that will degauss disks and tapes.

Burst—The separation of multiple-copy printout forms into individual sheets.

Bus—An electrical connection that allows two or more wires or lines to be connected together. Typically, all circuit cards receive the same information that is put on the bus, but only the card the information is "addressed" to will use that data.

Bus structure—A network topology in which nodes are connected to a single cable with terminators at each end.

Business Associate—Under HIPAA, a person who is not a member of a covered entity's workforce (see Workforce) and who performs any function or activity involving the use or disclosure of individually identifiable health information, such as temporary nursing services, or who provides services to a covered entity which involves the disclosure of individually identifiable health information, such as legal, accounting, consulting, data aggregation, management, accreditation, etc. A covered entity may be a business associate of another covered entity.

Business Continuity Plan (BCP)—A documented and tested plan for responding to an emergency.

Business Impact Analysis—An exercise that determines the impact of losing the support of any resource to an organization, establishes the escalation of that loss over time, identifies the minimum resources needed to recover and prioritizes the recovery of processes and supporting systems.

Business intelligence—Knowledge about customers, competitors, partners, and own internal operations. Business intelligence from information.

Business Model— A model of a business organization or process.

Business Partner (BP)— See Business Associate.

Business process—A standardized set of activities that accomplishes a specific task such as processing a customer's order.

Business Process Reengineering (BPR)—The reinventing of a process within a business.

Business Relationships—(a) The term agent is often used to describe a person or organization that assumes some of the responsibilities of another one. This term has been avoided in the final rules so that a more HIPAA-specific meaning could be used for business associate. The term business partner (BP) was originally used for business associate.

(b) A Third-Party Administrator (TPA) is a business associate that performs claims administration and related business functions for a self-insured entity.

(c) Under HIPAA, a healthcare clearinghouse is a business associate that translates data to or from a standard format on behalf of a covered entity.

(d) The HIPAA Security NPRM used the term Chain of Trust Agreement to describe the type of contract that would be needed to extend the responsibility to protect healthcare data across a series of sub-contractual relationships.

(e) A business associate is an entity that performs certain business functions for you, and a trading partner is an external entity, such as a customer, with whom you do business. This relationship can be formalized via a trading partner agreement. It is quite possible to be a trading partner of an entity for some purposes, and a business associate of that entity for other purposes.

Business requirement—A detailed knowledge worker request that the system must meet to be successful.

Business to business (B2B)—Companies whose customers are primarily other businesses.

Business to consumer (B2C)—Companies whose customers are primarily individuals.

Buyer agent or shopping bot—An intelligent agent or application on a Web site that helps customers find the products and services they want.

Byte—The basic unit of storage for many computers; typically, one configuration consists of 8 bits used to represent data plus a parity bit for checking the accuracy of representation.

Byte–digit portion—Usually, the four rightmost bits in a byte.

C—A third-generation computer language used for programming on microcomputers. Most microcomputer software products such as spreadsheets and DBMS programs are written in C.

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

C2—A formal product rating awarded to a product by the National Computer Security Center (NCSC). A C2 rated system incorporates controls capable of enforcing access limitations on an individual basis, making users individually accountable for their actions through logon procedures, auditing of security relevant events, and resource isolation.

CA—Certificate authority.

Cable—Transmission medium of copper wire or optical fiber wrapped in a protective cover.

Cable modem—A device that uses a TV cable to deliver an internet connection.

Cabulance—A taxi cab that also functions as an ambulance.

Cache—Pronounced *cash*, a special high-speed storage mechanism. It can be either a reserved section of main memory or an independent highspeed storage device. Two types of caching are commonly used in personal computers: *memory caching* and *disk caching*. A memory cache, sometimes called a *cache store* or *RAM cache*, is a portion of memory made of high-speed static RAM (SRAM) instead of the slower and cheaper dynamic RAM (DRAM) used for main memory. Memory caching is effective because most programs access the same data or instructions over and over. Disk caching works under the same principle as memory caching, but instead of using high-speed SRAM, a disk cache uses conventional main memory. When data is found in the cache, it is called a *cache hit,* and the effectiveness of a cache is judged by its *hit rate*.

Call—Any connection (fixed or temporary) capable of transferring information between two or more users of a telecommunications system. In this context, a user may be a person or a machine. It is used for transmission of the content of communication. This term refers to circuit-switched calls only.

Callback—A procedure that identifies a terminal dialing into a computer system or network by disconnecting the calling terminal, verifying the authorized terminal against the automated control table, and then, if authorized, reestablishing the connection by having the computer system dial the telephone number of the calling terminal.

Caller Identification (CLID)—One of several custom local area signaling services (CLASS) provided by the local exchange carrier. The service that allows you to see the name and number of the person who is calling you.

Call-Identifying Information (CII)—Dialing or signaling information that identifies the origin, direction, destination or termination of each communication generated by means of any equipment, facility, service, or a telecommunications carrier.

CAP—CM capabilities.

Capability—A token used as an identifier for a resource such that possession of the token confers access rights for the resource.

Capacitor—Capacitors provide a means of storing electric charge so that it can be released at a specific time or rate. A capacitor acts as a battery but does not use a chemical reaction.

Capacity planning—Determining the future IT infrastructure requirements for new equipment and additional network capacity.

Cardano's grille—a method of concealing a message by which a piece of paper has several holes cut in it (the grille) and when it is placed over an innocent looking message the holes cover all but specific letters spelling out the message. It was named for its inventor Girolamo Cardano.

Carrier Sense Multiple Access/Collision Detection (CSMA/CD)—Also known as Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA).

Carrier Sense, Multiple Access (CSMA)—A multiple-station access scheme for avoiding contention in packet networks in which each station can sense the presence of carrier signals from other stations and thus avoid transmitting a packet that would result in a collision. *See also* collision detection.

Cathode-Ray Tube (CRT)—The display device for computer terminals, typically a television-like electronic vacuum tube.

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. (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. .

Cave (cave automatic virtual environment)—A special 3-D virtual reality room that can display images of other people and objects located in other cave's all over the world.

CBC—Cipher block chaining.

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

CBO— Congressional Budget Office or Cost Budget Office.

CBR—Constant bit rate.

CC—Common Criteria; see ISO/IEC 15408.

CCA—Vulnerability analysis, covert channel analysis.

CCF—Common cause failure.

CCITT—Consultative Committee for International Telegraph and Telephone.

CCITT—See Telecommunications Standardization Sector of the International Telecommunications Union (TSSUITU).

CCO—Cisco Connection Online.

CCP—Compression Control Protocol.

CCS—Common channel signaling.

CCTV—Closed-circuit television.

CD—CARRIER DETECT.

CDC— See the Centers for Disease Control and Prevention.

CDDI—Copper Distributed Data Interface.

CDP—Cisco Discovery Protocol.

CD-R (compact disc-recordable)—An optical or laser disc that offers one-time writing capability with about 700 MB or greater of storage.

CD-ROM—A compact disk, similar to an audio compact disk, which is used to store computer information (e.g., programs, data, or graphics).

CD-RW (compact disc-rewritable)—A CD that offers unlimited writing and updating capabilities.

CDT— See Current Dental Terminology.

CE— See Covered Entity.

CEFACT— See United Nations Centre for Facilitation of Procedures and Practices for Administration, Commerce, and Transport (UN/CEFACT).

Cell sites—A transmitter-receiver location, operated by the wireless service provider, through which radio links are established between the wireless system and the wireless unit.

Cellular service—Also known as cellular mobile telephone system. A wireless telephone system using multiple transceiver sites linked to a central computer for coordination.

CEN— European Center for Standardization, or Comité Européen de Normalisation.

Central Office of Record—Office of a federal department or agency that keeps (COR) records of accountable COMSEC material held by elements subject to its oversight.

Central processing unit (CPU)—The part of a computer that performs the logic, computation, and decision-making functions. It interprets and executes instructions as it receives them. PCs have one CPU, typically a single chip.

CEO—Chief executive officer.

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

CER—Crossover error rate.

CERN—European Laboratory for Particle Physics. Birthplace of the World Wide Web.

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

Certificate—A set of information which at least: identifies the certification authority issuing the certificate; unambiguously names or identifies its owner; contains the owner's public key and is digitally signed by the certification authority issuing it.

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

Certification—The acceptance of software by an authorized agent, usually after the software has been validated by the agent or its validity has been demonstrated to the agent.

Certification Agent—The individual(s) responsible for making a technical judgment of the system's compliance with stated requirements, identifying and assessing the risks associated with operating the system, coordinating the certification activities, and consolidating the final certification and accreditation packages.

Certification and Accreditation Plan—A plan delineating objectives, responsibilities, schedule, technical monitoring, and other activities in support of the C&A process.

Certification and Repair Center (CRC)—A U.S. Department of State (DoS) facility utilized by IM/SO/TO/OTSS departments for program activities.

Certification Authority (CA)—Provides to users a digital certificate that links the public key with some assertion about the user, such as identity, credit payment card number etc. Certification authorities may offer other services such as time-stamping, key management services and certificate revocation services. It can also be defined as an independent trusted source which attests to some factual element of information for the purposes of certifying information in the electronic environment.

Certification level—A combination of techniques and procedures used during a certification and accreditation process to verify the correctness and effectiveness of security controls in an information technology system. Security certification levels represent increasing levels of intensity and rigor in the verification process and include such techniques as reviewing and examining documentation; interviewing personnel; conducting demonstrations and exercises; conducting functional, regression, and penetration testing; and analyzing system design documentation. .

Certification package—Product of the certification effort documenting the detailed results of the certification activities. The certification package includes the security plan, developmental or operational certification test reports, risk assessment report, and certifier's statement.

Certification Path—A chain of certificates between any given certificate and its trust anchor (CA). Each certificate in the chain must be verifiable in order to validate the certificate at the end of the path; this functionality is critical to the usable PKI.

Certification Practices Statement—A statement of the certification authorities practices with respect to a wide range of technical, business and legal issues that may be used as a basis for the certification authorities contract with the entity to whom the certificate was issued.

Certification Requirements Review (CRR)—The review conducted by the DAA, Certifier, program manager, and user representative to review and approve all information contained in the System Security Authorization Agreement (SSAA). The CRR is conducted before the end of Phase 1.

Certification statement—The certifier's statement provides an overview of the security status of the system and brings together all of the information necessary for the DAA to make an informed, risk-based decision. The statement documents that the security controls are correctly implemented and effective in their application. The report also documents the security controls not implemented and provides corrective actions. .

Certification Test and Evaluation (CT&E)—Software and hardware security tests conducted during development of an IS.

Certifier—See Certification Authority.

Certifier—See Certification Agent.

CFO—Chief financial officer.

CFR or C.F.R.— Code of Federal Regulations.

CGI—Common gateway interface.

Chain of Custody—The identity of persons who handle evidence between the time of commission of the alleged offense and the ultimate disposition of the case. It is the responsibility of each transferee to ensure that the items are accounted for during the time that it is in their possession, that it is properly protected, and that there is a record of the names of the persons from whom they received it and to whom they delivered it, together with the time and date of such receipt and delivery.

Chain of Custody—The control over evidence. Lack of control over evidence can lead to it being discredited completely. Chain of custody depends upon being able to verify that evidence could not have been tampered with. This is accomplished by sealing off the evidence so that it cannot in any way be changed and providing a documentary record of custody to prove that the evidence was at all times under strict control and not subject to tampering.

Chain of Evidence—The "sequencing" of the chain of evidence follows this order: Collection and identification; Analysis; Storage; Preservation; Presentation in court; Return to owner. Chain of evidence shows: Who obtained the evidence; Where and when the evidence was obtained; Who secured the evidence; Who had control or possession of the evidence.

Chain of Trust (COT)—A term used in the HIPAA Security NPRM for a pattern of agreements that extend protection of healthcare data by requiring that each covered entity that shares healthcare data with another entity require that that entity provide protections comparable to those provided by the covered entity, and that that entity, in turn, require that any other entities with which it shares the data satisfy the same requirements.

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.

CHAMPUS—Civilian Health and Medical Program of the Uniformed Services.

Channel—Typically what you rent from the telephone company, voice-grade transmission facility with defined frequency response, gain, and bandwidth. A path of communication, either electrical or electromagnetic, between two or more points. Also a circuit, facility, line, or path.

Channel Service Unit (CSU) or Digital Service Unit (DSU)—Devices used to interface between transmitting equipment and the external circuit in the wide area network that will carry the information.

CHAP (Challenge Handshake Authentication Protocol)—Applies a three-way handshaking procedure. After the link is established, the server sends a "challenge" message to the originator. The originator responds with a value calculated using a one-way hash function. The server checks the response against its own calculation of the expected hash value. If the values match, the authentication is acknowledged; otherwise, the connection is usually terminated.

Character—A single numeric digit, special symbol, or letter.

Charging Data Record (CDR)—A formatted collection of information about a chargeable event (e.g., time of call set-up, duration of the call, amount of data transferred, etc.) for use in billing and accounting. For each party to be charged for parts of or all the charges of a chargeable event, a separate CDR shall be generated, i.e., more than one CDR may be generated for a single chargeable event, e.g., because of its long duration or because more than one charged party is to be charged.

Chat Room—An area of a Web chat service that people can "enter" with their Web browsers where the conversations are devoted to a specific topic; equivalent to a channel in IRC.

Check Digit—One digit, usually the last, of an identifying field is a mathematical function of all of the other digits in the field. This value can be calculated from the other digits in the field and compared with the check digit to verify validity of the whole field.

Check digit—A numeric digit that is used to verify the accuracy of a copied or transcribed number. The numeric digit is typically appended to the end of a number.

Checksum—A computed value that depends on the contents of a packet. This value is sent along with the packet when it is transmitted. The receiving system computes a new checksum based on receiving data and compares this value with the one sent with the packet. If the two values are the same, the receiver has a high degree of confidence that the data was received correctly.

Chief Information Officer (CIO)—The title for the highest-ranking MIS officer in the organization.

CHIM—See the Center for Healthcare Information Management.

CHIME—See the College of Healthcare Information Management Executives.

Chip—A wafer containing miniature electronic imprinted circuits and components.

CHIP—Child Health Insurance Program.

Choice—The third step in the decision-making process where you decide on a plan to address the problem or opportunity.

Chosen message attack—A type of attack where the steganalyst generates a stego-medium from a message using some particular tool, looking for signatures that will enable the detection of other stego-media.

Chosen stego attack—A type of attack when both the stego-medium and the steganography tool or algorithm is available.

CIA—With regard to information security; Confidentiality, Integrity and Availability.

CIDF—Common intrusion detection framework model.

CIDR—Classless interdomain routing.

CIO—Chief information officer.

Cipher disk—An additive cipher device used for encrypting and decrypting messages. The disk consists of two concentric circular scales, usually of letters, and the alphabets can be repositioned with respect to one another at any of the 26 relationships.

Cipher system—A system in which cryptography is applied to plaintext elements of equal length.

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

Ciphertext—Information that has been encrypted, making it unreadable without knowledge of the key.

CIR—Committed information rate.

Circuit Switching—A communications paradigm in which a dedicated communication path is established between two hosts and on which all packets travel. The telephone system is an example of a circuit-switched network.

CISL—Common Intrusion Specification Language.

CISM—Certified Information Security Manager.

CISO—Chief information security officer.

CISSP—Certified Information Systems Security Professional.

CKM—Cryptographic key management.

Claim Adjustment Reason Codes—A national administrative code set that identifies the reasons for any differences, or adjustments, between the original provider charge for a claim or service and the payer's payment for it. This code set is used in the X12 835 Claim Payment & Remittance Advice and the X12 837 Claim transactions, and is maintained by the Health Care Code Maintenance Committee.

Claim Attachment— Any of a variety of hardcopy forms or electronic records needed to process a claim in addition to the claim itself.

Claim authentication information—Information used by a claimant to generate exchange AI needed to 874 authenticate a principal.

Claim Medicare Remark Codes— See Medicare Remittance Advice Remark Codes.

Claim Status Category Codes— A national administrative code set that indicates the general category of the status of healthcare claims. This code set is used in the X12 277 Claim Status Notification transaction, and is maintained by the Health Care Code Maintenance Committee.

Claim Status Codes— A national administrative code set that identifies the status of healthcare claims. This code set is used in the X12 277 Claim Status Notification transaction, and is maintained by the Health Care Code Maintenance Committee.

Claimant—An entity which is or represents a principal for the purposes of authentication. A claimant includes the functions necessary for engaging in authentication exchanges on behalf of a principal.

Class—An implementation of an abstract data type. A definition of the data structures, methods, and interface of software objects. A template for the instantiation (creation) of software objects.

Classification—The determination that certain information requires protection against unauthorized disclosure in the interest of national security, coupled with the designation of the level of classification Top Secret, Secret, or Confidential.

Classification Authority—The authority vested in an official of an agency to originally classify information or material which is determined by that official to require protection against unauthorized disclosure in the interest of national security.

Classification Guides—Documents issued in an exercise of authority for original classification that include determinations with respect to the proper level and duration of classification of categories of classified information.

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.

Classifier—An individual who makes a classification determination and applies a security classification to information or material. A classifier may either be a classification authority or may assign a security classification based on a properly classified source or a classification guide.

Clear mode—Unencrypted plain text mode.

Cleared U.S. citizen—A citizen of the United States who has undergone a favorable background investigation resulting in the issuance of a security clearance by the Bureau of Diplomatic Security permitting access to classified information at a specified level.

Clearinghouse— See Health Care Clearinghouse.

Cleartext—Data that is not encrypted; plaintext.

CLIA— Clinical Laboratory Improvement Amendments.

Click trail—A record of all the Web page addresses you have visited during a specific online session. Click trails tell not just what Web site you visited, but which pages inside that site. .

Clickstream—A stored record of a Web surfing session containing information such as Web sites visited, how long the user was there, what ads were looked at, and the items purchased.

Click-throughs—A count of the number of people who visit one site and click on an ad, and are taken to the site of the advertiser.

Client—A workstation in a network that is set up to use the resources of a server.

Client/Server—In networking, a network in which several PC-type systems (clients) are connected to one or more powerful, central computers (servers). In databases, refers to a model in which a client system runs a database application (front end) that accesses information in a database management system situated on a server (back end).

Client/Server Architecture—A local area network in which microcomputers, called servers, provide specialized service on behalf of the user's computers, which are called clients.

Client/Server Model—A common way to describe network services and the model user processes (programs) of those services. Examples include the name-serve/name-resolver paradigm of the DNS and file-server/file-client relationships such as NFS and diskless hosts.

Clinger–Cohen Act of 1996—Also known as the Information Technology Management Reform Act. A statute that substantially revised the way that information technology resources are managed and procured, including a requirement that each agency design and implement a process for maximizing the value and assessing and managing the risks of information technology investments. .

Clinical Code Sets—See Medical Code Sets.

CLNP—Connectionless Network Protocol.

CLNS—Connectionless Network Services.

Cloning—The term given to the operation of creating an exact duplicate of one medium on another like medium. This is also referred to as a Mirror Image or Physical Sector Copy.

Closed network/closed user group—These are systems which generally represent those in which certificates are used within a bounded context such as within a payment system. A contract or series of contracts identify and define the rights and responsibilities of all parties to a particular transaction.

CLP—Cell loss priority.

CM— See ICD.

CMF—Common mode failure.

CMI—Coded mark inversion.

CO—Central office.

Coaxial Cable—A medium used for telecommunications. It is similar to the type of cable used for carrying television signals.

COB— See Coordination of Benefits.

COBOL—See Common Business-Oriented Language.

Code Division Multiple Access (CDMA)—A technique permitting the use of a single frequency band by a number of users. Users are allocated a sequence that uniquely identifies them.

Code generator—A precompiler program that translates fourth-generation language-like code into the statements of a third-generation language code.

Code of fair information practices—The basis for privacy best practices, both online and offline. The practices originated in the Privacy Act of 1974, the legislation that protects personal information collected and maintained by the U.S. Government. In 1980, these principles were adopted by the Organization for Economic Cooperation and Development and incorporated in its Guidelines for the Protection of Personal Data and Transborder Data Flows. They were adopted later in the EU Data Protection Directive of 1995, with modifications. The Fair Information Practices include notice, choice, access, onward transfer, security, data integrity, and remedy. .

Code Room—The designated and restricted area in which cryptographic operations are conducted.

Code Set—Under HIPAA, this is any set of codes used to encode data elements, such as tables of terms, medical concepts, medical diagnostic codes, or medical procedure codes. This includes both the codes and their descriptions. Also see Part II, 45 CFR 162.103.

Code Set Maintaining Organization—Under HIPAA, this is an organization that creates and maintains the code sets adopted by the secretary for use in the transactions for which standards are adopted. Also see Part II, 45 CFR 162.103.

Code System—Any system of communication in which groups of symbols represent plaintext elements of varying length.

Coder—The individual who translates program design into executable computer code.

Coding—The activity of translating a set of computer processing specifications into a formal language for execution by a computer.

Coefficient—a number or symbol multiplied with a variable or an unknown quantity in an algebraic term.

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.

Cold Site—An IS backup facility that has the necessary electrical and physical components of a computer facility, but does not have the computer equipment in place. The site is ready to receive the necessary replacement computer equipment in the event the users have to move from their main computing location to the alternative computer facility.

Collaboration—Enabling collaboration which transforms shared awareness into actions which can achieve a competitive advantage.

Collaboration System—A system that is designed specifically to improve the performance of teams by supporting the sharing and flow of information.

Collaborative Filtering—A method of placing you in an affinity group of people with the same characteristics.

Collaborative Planning, Forecasting, and Replenishment (CPFR)—A concept that encourages and facilitates collaborative processes between members of a supply chain.

Collaborative Processing Enterprise Information Portal—Provides knowledge workers with access to workgroup information such as e-mails, reports, meeting minutes, and memos.

Collateral Information—National security information classified in accordance with E.O. 12356, dated April 2, 1982.

College of Healthcare Information Management Executives (CHIME)—A professional organization for healthcare Chief Information Officers (CIOs).

Collision—(1) A condition that is present when two or more terminals are in contention during simultaneous network access attempts. (2) In cryptography, an instance when a hash function generates the same output for different inputs.

Collision Detection—An avoidance method for communications channel contention that depends on two stations detecting the simultaneous start of each other's transmission, stopping, and waiting a random period of time before beginning again. See also *carrier sense, multiple access.*

Collision Resistance —In cryptography, the idea that a hash function does not generate the same output for different inputs. Consider for example.

Co-location—A vendor that rents space and telecommunications equipment to other companies.

Color palette—A set of available colors a computer or an application can display. Also known as a *CLUT*: Color Look Up Table.

COM (computer output microfilm)—The production of computer output on photographic film.

Command and Control—The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission.

Command and Control Warfare (C2W)—The integrated use of operations security (OPSEC), military deception, psychological operations (PSYOP), electronic warfare (EW) and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade or destroy adversary C2 capabilities, while protecting friendly C2 capabilities against such actions.

Comment— Public commentary on the merits or appropriateness of proposed or potential regulations provided in response to an NPRM, an NOI, or other federal regulatory notice.

Commit—A condition implemented by the programmer signaling to the DBMS that all update activity that the program conducts be executed against a database. Before the commit, all update activity can be rolled back or canceled without negative impact on the database contents.

Commit Protocol—An algorithm to ensure that a transaction is successfully completed.

Common Business Oriented Language (COBOL)—A high-level programming language for business computer applications.

Common carrier—An organization or company that provides data or other electronic communication services for a fee.

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

Common Control— See HIPPA Part II, 45 CFR 164.504.

Common Criteria Testing Laboratory (CCTL)—Within the context of the NIAP Common Criteria Evaluation and Validation Scheme, an IT security evaluation facility, accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the NIAP Oversight Body to conduct CC-based evaluations.

Common mode failure—Failure of multiple independent system components that fail in the identical mode.

Common Object Request Broker Architecture (CORBA)—CORBA is the Object Management Group's (OMG) answer to the need for interoperability among the rapidly proliferating number of hardware and software products available today. Simply stated, CORBA allows applications to communicate with one another no matter where they are located or who has designed them.

Common Operating Environment—The collection of standards, specifications, and guidelines, architecture definitions, software infrastructures, reusable components, application programming interfaces (APIs), methodology, runtime environment definitions, reference implementations, and methodology, that establishes an environment on which a system can be built. The COE is the vehicle that assures interoperability through a reference implementation that provides identical implementation of common functions. It is important to realize that the COE is both a standard and an actual product.

Common Ownership— See Part II, 45 CFR 164.504.

Common security control—A security control that can be applied to one or more organization information systems and has the following properties: (1) the development, implementation, and assessment of the control can be assigned to a responsible official or organizational element (other than the information system owner); and (2) the results from the assessment of the control can be used to support the security certification and accreditation processes of an organization information system where that control has been applied. .

Communication—Information transfer according to agreed conventions.

Communication Protocols—A set of rules that govern the operation of hardware or software entities to achieve communication.

Communications medium—The path or physical channel in a network over which information travels.

Communications Protocol (protocol)—A set of rules that every computer follows to transfer information.

Communications satellite—A microwave repeater in space.

Communications Security—The protection that ensures the authenticity of telecommunications and that results from the application of measures taken to deny unauthorized persons access to valuable information that might be derived from the acquisition of telecommunications.

Communications service provider—A third party who furnishes the conduit for information.

Communications software—Helps you communicate with other people.

Communications System—A mix of telecommunications and automated information systems used to originate, control, process, encrypt, and transmit or receive information. Such a system generally consists of the following connected or connectable devices (1) Automated information equipment (AIS) on which information is originated; (2) A central controller (i.e., CIHS, C-LAN) of, principally, access rights and information distribution; (3) A telecommunications processor (i.e., TERP, IMH) which prepares information for transmission; and (4) National-level devices which encrypt information (COMSEC/CRYPTO/CCI) prior to its transmission via Diplomatic Telecommunications Service (DTS) or commercial carrier.

Companding—The process where there is a greater number of samples provided at lower power conditions of the signal waveform rather than at the higher power portions of the same waveform.

Compare—A computer-applied function that examines two elements of data to determine their relationship to one another.

Compartmentalization—The isolation of the operating system, user programs, and data files from one another in main storage to protect them against unauthorized or concurrent access by other users or programs. Also, the division of sensitive data into small, isolated blocks to reduce risk to the data.

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: (1) valid security clearance for the most restricted information processed in the system; (2) formal access approval and signed nondisclosure agreements for that information which a user is to have access; and (3) valid need-to-know for information that a user is to have access.

Competitive advantage—Providing a product or service in a way that customers value more than what the competition is able to do.

Competitive Local Exchange Carriers (CLEC)—A competitive access provider that also provides switched local services, such as local dial tone and Centrex. CLEC are authorized by state commissions to resell existing incumbent LEC services at wholesale rates and lease component facilities for use with their own facilities.

Compiler—A program that translates high-level computer language instructions into machine code.

Complementor—Provides services that complement the offerings of the enterprise and thereby extend its value-adding capabilities to its customers.

Completeness—The property that all necessary parts of an entity are included. Completeness of a product often means that the product has met all requirements.

Compliance Date— Under HIPAA, this is the date by which a covered entity must comply with a standard, an implementation specification, or a modification. This is usually 24 months after the effective data of the associated final rule for most entities, but 36 months after the effective data for small health plans. For future changes in the standards, the compliance date would be at least 180 days after the effective data, but can be longer for small health plans and for complex changes. Also see Part II, 45 CFR 160.103.

Component—Basic unit designed to satisfy one or more functional requirements.

Composite primary key—The primary key fields from two intersecting relations.

Composite Threat List—A Department of State threat list intended to cover all localities operating under the authority of a chief of mission and staffed by direct-hire U.S. personnel. This list is developed in coordination with the intelligence community and issued semiannually by the Bureau of Diplomatic Security.

Compression—a method of storing data in a format that requires less space than normal. .

Compromise—Unauthorized disclosure or loss of sensitive information.

Compromising Emanations—Electromagnetic emanations that convey data and that, if intercepted and analyzed, could compromise sensitive information being processed by a computer system.

COMPUSEC—Computer security.

Computer—The hardware, software, and firmware components of a system that are capable of performing calculations, manipulations, or storage of data. It usually consists of arithmetic, logical, and control units, and may have input, output, and storage devices.

Computer crime—The act of using IT to commit an illegal act.

Computer Emergency Response Team (CERT)—The CERT is chartered to work with the Internet community to facilitate its response to computer security events involving Internet hosts, to take proactive steps to raise the community's awareness of computer security issues, and to conduct research targeted at improving the security of existing systems. The U.S. CERT is based at

Carnegie Mellon University in Pittsburgh; regional CERTs are like NICs, springing up in different parts of the world.

Computer ethics—The issues and standards that support the proper use of IT which are not criminal or threatening to another person or organization.

Computer Evidence—Computer evidence is a copy of a document stored in a computer file that is identical to the original. The legal "best evidence" rules change when it comes to the processing of computer evidence. Another unique aspect of computer evidence is the potential for unauthorized copies to be made of important computer files without leaving behind a trace that the copy was made. This situation creates problems concerning the investigation of the theft of trade secrets (e.g., client lists, research materials, computer-aided design files, formulas, and proprietary software).

Computer Forensics—The term "computer forensics" was coined in 1991 in the first training session held by the International Association of Computer Specialists (IACIS) in Portland, Oregon. Since then, computer forensics has become a popular topic in computer security circles and in the legal community. Like any other forensic science, computer forensics deals with the application of law to a science. In this case, the science involved is computer science and some refer to it as Forensic Computer Science. Computer forensics has also been described as the autopsy of a computer hard disk drive because specialized software tools and techniques are required to analyze the various levels at which computer data is stored after the fact. Computer forensics deals with the preservation, identification, extraction, and documentation of computer evidence. The field is relatively new to the private sector, but it has been the mainstay of technology-related investigations and intelligence gathering in law enforcement and military agencies since the mid-1980s. Like any other forensic science, computer forensics involves the use of sophisticated technology tools and procedures that must be followed to guarantee the accuracy of the preservation of evidence and the accuracy of results concerning computer evidence processing. Typically, computer forensic tools exist in the form of computer software.

Computer Fraud and Abuse Act PL 99-474—Computer Fraud and Abuse Act of 1986. Strengthens and expands the 1984 Federal Computer Crime Legislation. Law extended to computer crimes in private enterprise and anyone who willfully disseminates information for the purpose of committing a computer crime (i.e., distribute phone numbers to hackers from a BBS).

Computer Matching Act (P.L. 100-503)—The Computer Matching and Privacy Act of 1988 ensures privacy, integrity, and verification of data disclosed for computer matching and establishes data integrity boards within federal agencies.

Computer Matching Act Public Law (PL) 100-53—Computer Matching and Privacy Act of 1988. Ensures privacy, integrity, and verification of data disclosed for computer matching; establishes Data Integrity Boards within federal agencies.

Computer network—Two or more computers connected so that they can communicate with each other and share information, software, peripheral devices, and processing power.

Computer Output Microfilm (COM)—The production of computer output on photographic film.

Computer program—A series of operations that perform a task when executed in logical sequence.

Computer Security—The practice of protecting a computer system against internal failures, human error, attacks, and natural catastrophes that might cause improper disclosure, modification, destruction, or denial-of-service.

Computer Security Act PL 100-235—Computer Security Act of 1987 directs the National Bureau of Standards (now the National Institute of Standards and Technology [NIST]) to establish a computer security standards program for federal computer systems.

Computer System—An interacting assembly of elements, including at least computer hardware and usually software, data procedures, and people.

Computer System Security—All of the technological safeguards and managerial procedures established and applied to computers and their networks (including related hardware, firmware, software, and data) to protect organizational assets and individual privacy.

Computer virus—Software that is written with malicious intent to cause annoyance or damage.

Computer-Aided Design (CAD)—A term used to describe the use of computer technology as applied to the design of problems and opportunities.

Computer-Aided Instruction (CAI)—The interactive use of a computer for instructional purposes. Software provides educational content to students and adjusts its presentation to the responses of the individual.

Computer-Aided Manufacturing (CAM)—The use of computer technology as applied to the manufacturing of computer technology as applied to the manufacturing of goods and services.

Computer-Aided Software Engineering (CASE)—Tools that automate the design, development, operation, and maintenance of software.

Computer-Based Patient Record Institute (CPRI)—Healthcare Open Systems and Trials (HOST)— An industry organization that promotes the use of healthcare information systems, including electronic healthcare records.

Computing Environment—The total environment in which an automated information system, network, or component operates. The environment includes physical, administrative, and personnel procedures as well as communication and networking relationships with other information systems.

COMSEC—Communications security.

COMSEC Account—Administrative entity, identified by an account number, used to maintain accountability, custody, and control of COMSEC material.

COMSEC Custodian—Person designated by proper authority to be responsible for the receipt, transfer, accounting, safeguarding, and destruction of COMSEC material assigned to a COMSEC account.

COMSEC Facility—Space used for generating, storing, repairing, or using COMSEC material.

COMSEC Manager—Person who manages the COMSEC resources of an organization.

COMSEC Material—Item designed to secure or authenticate telecommunications. COMSEC material includes, but is not limited to key, equipment, devices, documents, firmware, or software that embodies or describes cryptographic logic and other items that perform COMSEC function.

COMSEC Material Control System (CMCS)—Logistics and accounting system through which COMSEC material marked “CRYPTO” is distributed, controlled, and safeguarded. Included are the COMSEC central offices of record, crypto-logistic depots, and COMSEC accounts. .

COMSEC Officer—The properly appointed individual responsible to ensure that COMSEC regulations and procedures are understood and adhered to, that the COMSEC facility is operated securely, that personnel are trained in proper COMSEC practices, and who advises on communications security matters. Only Department of State personnel will be appointed.

Concealment Systems—A method of keeping sensitive information confidential by embedding it in irrelevant data.

Concentrator—A computer that consolidates the signals from any slower speed transmission lines into a single faster line or performs the reverse function.

Concurrent Processing—The capability of a computer to share memory with several programs and simultaneously execute the instructions provided by each.

Condensation—The process of reducing the volume of data managed without reducing the logical consistency of data. It is essentially different than compaction in that condensation is done at the record level whereas compaction is done at the system level.

Condition test—A comparison of two data items in a program to determine whether one value is equal to, less than, or greater than the second value.

Conditional branch—The alteration of the normal sequence of program execution following the text of the contents of a memory area.

Conditional formatting—Highlights the information in a cell that meets some specified criteria.

Conductor—A material that allows the easy transfer of electrons from one atom to another.

Conference on Data Systems Languages (CODASYL)—A Department of Defense-sponsored group that studies the requirements and design specifications for a common business programming language.

Confidence—Confidence in electronic interactions can be significantly increased by solutions that address the basic requirements of integrity, confidentiality, authentication, authorization and access management or access control.

Confidentiality—A concept that applies to data that must be held in confidence and describes that status or degree of protection that must be provided for such data about individuals as well as organizations.

Confidentiality Loss—The compromise of sensitive, restricted, or classified data or software.

Configuration Control—The process of controlling modifications to the system's hardware, firmware, software, and documentation that provides sufficient assurance that the system is protected against the introduction of improper modifications prior to, during, and after system implementation. Compare configuration management.

Configuration Management—The use of procedures appropriate for controlling changes to a system's hardware, software, or firmware structure to ensure that such changes will not lead to a weakness or fault in the system.

Configuration Manager—The individual or organization responsible for configuration control or configuration management.

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. (2) Restricting an untrusted program from accessing system resources and executing system processes. Common confinement techniques include DTE, least privilege, and wrappers.

Connected mode—The state of user equipment switched on and an RRC connection established.

Connection—A communication channel between two or more endpoints (e.g., terminal, server, etc.).

Connectionless—The model of interconnection in which communication takes place without first establishing a connection. Sometimes (imprecisely) called datagram. Examples: Internet IP and OSI CLNP, UDP, ordinary postcards.

Connection-Oriented—The model of interconnection in which communication proceeds through three well-defined phases: connection establishment, data transfer, and connection release. Examples: X.25, Internet TCP and OSI TP4, ordinary telephone calls.

Connectivity—The uninterrupted availability of information paths for the effective performance of C2 functions.

Connectivity software—Enables a computer to "dial up" or connect to another computer.

Consent—Explicit permission, given to a Web site by a visitor, to handle her personal information in specified ways. Web sites that ask users to provide personally identifiable information should be required to obtain "informed consent," which implies that the company fully discloses its information practices prior to obtaining personal data or permission to use it. .

Consistency—Logical coherency among all integrated parts; also, adherence to a given set of instructions or rules.

Console Operator—Someone who works at a computer console to monitor operations and initiate instructions for efficient use of computer resources.

Constant—A value in a computer program that does not change during program execution.

Construct—An object; especially a concept that is constructed or synthesized from simple elements.

Consumer Electronics—Any electronic/electrical devices, either AC- or battery-powered, which are not part of the facility infrastructure. Some examples are radios, televisions, electronic recording or playback equipment, PA systems, paging devices, and dictaphones (see also electronic equipment).

Consumers—Traditionally, the ultimate user or consumer of goods, ideas, and services. However, the term also is used to imply the buyer or decision maker as well as the ultimate consumer. A mother buying cereal for consumption by a small child is often called the consumer although she may not be the ultimate user. .

Content—See Completeness.

Content of Communication (CC)—Information exchanged between two or more users of a telecommunications service, excluding intercept related information (IRI). This includes information which may, as part of some telecommunications service, be stored by one user for subsequent retrieval by another.

Content of communication link—A communication channel for HI3 information between a mediation function and an LEMF.

Contention—Occurs during multiple access to a network in which the network capacity is allocated on a "first come, first served" basis.

Contextual information—Information derived from the context in which an access is made (for example, time of day).

Contingency Plans—Plans for emergency response, backup operations, and post-disaster recovery maintained by a computer information processing facility as a part of its security program.

Continuity—The uninterrupted availability of information paths for the effective performance of organizational function.

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

Contrary—See Part II, 45 CFR 160.202.

Control—Any protective action, device, procedure, technique, or other measure that reduces exposures.

Control Break—A point during program processing at which some special processing event takes place. A change in the value of a control field within a data record is characteristic of a control break.

Control field—A field of data within a record used to identify and classify a record.

Control logic—The specific order in which processing functions are carried out by a computer.

Control signals—Computer-generated signals for the automatic control of machines and processes.

Control statement—A command in a computer program that establishes the logical sequence of processing operations.

Control structure—A program that contains a logical construct of sequences, repetitions, and selections.

Control Totals—Accumulations of numeric data fields that are used to check the accuracy of the input, processing, or output data.

Control unit—A component of the CPU that evaluates and carries out program processing and execution.

Control Zone—The space surrounding equipment that is used to process sensitive information and that is under sufficient physical and technical control to preclude an unauthorized entry or compromise.

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.).

Controllable isolation—Controlled sharing in which the scope or domain of authorization can be reduced to an arbitrarily small set or sphere of activity.

Controlled Access Area—Controlled access areas are specifically designated areas within a building where classified information may be handled, stored, discussed, or processed.

Controlled Cryptographic Item (CCI)—Secure telecommunications or information handling equipment, or associated cryptographic components, which are unclassified but governed by a special set of control requirements.

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.

Controlled sharing—The condition that exists when access control is applied to all users and components of a resource-sharing computer system.

Controlled Shipment—The transport of material from the point at which the destination of the material is first identified for a site, through installation and use, under the continuous 24-hour control of Secret cleared U.S. citizens or by DS-approved technical means and seal.

Conversational program—A program that permits interaction between a computer and a user.

Conversion—The process of replacing a computer system with a new one.

Conversion rate—The percentage of customers who visit a Web site and actually buy something.

Cookie—A cookie is a piece of text that a Web server can store on a user's hard disk. Cookies allow a Web site to store information on a user's machine and later retrieve it. The pieces of information are stored as name-value pairs.

Cooperative Processing—The ability to distribute resources (i.e., programs, files, and databases) across the network.

Coordination of Benefits (COB)—A process for determining the respective responsibilities of two or more health plans that have some financial responsibility for a medical claim. Also called cross-over.

COP—Cryptographic operation.

Copy—An accurate reproduction of information contained on an original physical item, independent of the original physical item.

Copyright—The author or artist's right to control the copying of his or her work.

CORBA—Common Object Request Broker Architecture, introduced in 1991 by the OMG, defined the Interface Definition Language (IDL) and the Application Programming Interfaces (APIs) that enable client/server object interaction within a specific implementation of an Object Request Broker (ORB).

CORBA security—The Object Management Group standard that describes how to secure CORBA environments.

CORF—Comprehensive Outpatient Rehabilitation Facility.

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

Corrective Action—The practice and procedure for reporting, tracking, and resolving identified problems, in both the software product and the development process. Their resolution provides a final solution to the identified problem.

Corrective Maintenance—The identification and removal of code defects.

Correctness—The extent to which software is free from design and coding defects (i.e., fault free). Also, the extent to which software meets its specified requirements and user objectives.

Corruption—Departure from an original, correct data file or correctly functioning system to an improper state.

Cost/Benefit Analysis—Determination of the economic feasibility of developing a system on the basis of a comparison of the projected costs of a proposed system and the expected benefits from its operation.

Cost-Risk Analysis—The assessment of the cost of potential risk of loss or compromise of data in a computer system without data protection versus the cost of providing data protection.

COT—See Chain of Trust.

COTS—Commercial off-the-shelf software.

Counterfeit software—Software that is manufactured to look like the real thing and sold as such.

Counterfeits—Duplicates that are copied and packaged to resemble the original as closely as possible. The original producer's trademarks and logos are reproduced in order to mislead the consumer into believing that they are buying an original product.

Countermeasure—The deployment of a set of security services to protect against a security threat.

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.

Courseware—Computer programs used to deliver educational materials within computer-assisted instruction systems.

COV—Tests, coverage.

Cover escrow—An extraction process method that needs both the original piece of information and the encoded one in order to extract the embedded data. .

Cover medium—The medium in which we want to hide data; it can be an innocent looking piece of information for steganography, or an important medium that must be protected for copyright or integrity reasons.

Covered Entity—The specific types of organizations to which HIPAA applies, including providers, health plans (payers), and clearinghouses (who process nonstandard claims from providers and distribute them to the payers in their required formats--a process that will not be necessary if providers adopt the HIPAA transactions standards).

Covered Function—Functions that make an entity a health plan, a healthcare provider, or a healthcare clearinghouse. Also see Part II, 45 CFR 164.501.

Covert channel—A channel of communication within a computer system, or network, which is not designed or intended to transfer information.

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.

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.

CPE—Customer premise equipment.

CPRI—Computer-based Patient Record Institute--organization formed in 1992 to promote adoption of healthcare information systems. Has created a Security Toolkit with sample policies and procedures.

CPRI-HOST—See the Computer-Based Patient Record Institute—Healthcare Open Systems and Trials.

CPT—See Current Procedural Terminology.

CPU—The central processing unit; the brains of the computer.

Cracker—The correct name for an individual who hacks into a networked computer system with malicious intentions. The term hacker is used interchangeably (although incorrectly) because of media hype of the word hacker. A cracker explores and detects weak points in the security of a computer networked system and then exploits these weaknesses using specialized tools and techniques.

Crash-proof software—Utility software that helps save information if the system crashes and the user is forced to turn it off and then back on.

CRC—Cyclical redundancy check.

Credentials—Data that is transferred to establish the claimed identity of an entity.

Critical Path—A tool used in project management techniques and is the duration based on the sum of the individual tasks and their dependencies. The critical path is the shortest period in which a project can be accomplished.

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.

Critical Success Factor (CSF)—A factor simply critical to the organization’s success.

Criticality—The severity of the loss of either data or system functionality. Involves judicious evaluation of system components and data when a property or phenomenon undergoes unwanted change.

Criticality Analysis—An analysis or assessment of a business function or security vulnerability based on its criticality to the organization's business objectives. A variety of criticality may be used to illustrate the criticality.

CRL—Certificate revocation list.

Cross Certification—Practice of mutual recognition of another certification authority is certificates to an agreed level of confidence. Usually evidenced in contract.

Crossover—The process within a genetic algorithm where portions of the good outcome are combined in the hope of creating an even better outcome.

Crossover Error Rate (CER)—A comparison metric for different biometric devices and technologies; the error rate at which FAR equals FRR. The lower the CER, the more accurate and reliable the biometric device.

Crosstalk—An unwanted transfer of energy from one communications channel to another.

Cross-Walk—See Data Mapping.

CRT—A monitor that looks like a television set.

CRUD (create, read, update, delete)—The four primary procedures or ways a system can manipulate information.

Cryptanalysis—The study of techniques for attempting to defeat cryptographic techniques and, more generally, information security services.

Cryptanalyst—Someone who engages in cryptanalysis.

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 Ignition Key (CIK)—The device or electronic key used to unlock the secure mode of crypto equipment.

Cryptographic Access—The prerequisite to, and authorization for, access to crypto information, but does not constitute authorization for use of crypto equipment and keying material issued by the Department.

Cryptographic algorithm—A method of performing a cryptographic transformation (see cryptography) on a data unit. Cryptographic algorithms may be based on symmetric key methods (the same key is used for both encipher and decipher transformations) or on asymmetric keys (different keys are used for encipher and decipher transformations).

Cryptographic Checkvalue—Information that is derived by performing a cryptographic transformation on a data unit.

Cryptographic key—A parameter used with a cryptographic algorithm to transform, validate, authenticate, encrypt or decrypt data.

Cryptographic Material—All COMSEC material bearing the marking "CRYPTO" or otherwise designated as incorporating cryptographic information.

Cryptographic System—The documents, devices, equipment, and associated techniques that are used as a unit to provide a single means of encryption.

Cryptography—The study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication. Cryptography is not the only means of providing information security services, but rather one set of techniques. The word itself comes from the Greek word *kryptos,* which means "hidden" or "covered." Cryptography is a way to hide writing but yet retain a way to uncover it again.

Cryptology—The science that deals with hidden, disguised, or encrypted communications. It embraces communications security and communications intelligence.

Cryptolope—An IBM product which means "cryptographic envelope". Cryptolope objects are used for secure, protected delivery of digital content by using encryption and digital signatures.

Cryptosystem—A general term referring to a set of cryptographic primitives used to provide information security services.

CSI—Computer Security Institute.

CSMA/CD—Carrier Sense Multiple Access/Collision Detect.

CSNP—Complete Sequence Number PDU.

CSPDN—Circuit-switched public data network.

CSU/DSU—Channel service unit/digital service unit.

CTS—Clear to send.

CUD—Caller user data (X.25).

Culture—The collective personality of a nation, society, or organization, encompassing language, traditions, currency, religion, history, music, and acceptable behavior, among other things.

Current—A measure of how much electricity passes a point on a wire in a given time frame. Current is measured in amperes or amps.

Current Dental Terminology (CDT)—A medical code set, maintained and copyrighted by the ADA, that has been selected for use in the HIPAA transactions.

Current Procedural Terminology (CPT)—A medical code set, maintained and copyrighted by the AMA, that has been selected for use under HIPAA for non-institutional and non-dental professional transactions.

Custodian—An individual who has possession of or is otherwise charged with the responsibility for safeguarding and accounting for classified information.

Custom auto filter function—Allows one to hide all the rows in a list except those that match criteria specified.

Customer Relationship Management (CRM)—CRM entails all aspects of service and sales interactions a company has with its customer. CRM often involves personalizing online experiences, help-desk software, and e-mail organizers.

Customer-integrated system—An extension of a TPS that places technology in the hands of an organization's customers and allows them to process their own transactions.

Customers—The actual or prospective purchaser of products or services. .

Cybercops—A criminal investigator of online fraud or harassment.

Cybercrime—A criminal offense that involves the use of a computer network.

Cyberspace—Refers to the connections and locations (even virtual) created using computer networks. The term "Internet" has become synonymous with this word.

Cyberterrorist—One who seeks to cause harm to people or destroy critical systems or information.

Cycle—One complete sequence of an event or activity. Often refers to electrical phenomena. One electrical cycle is a complete sine wave.

Cyclical Redundancy Check (CRC)—A process used to check the integrity of a block of data. It provides an integrity check of the data before it is sent out into the wide area network. Its value depends on the hexadecimal value of the number of 1s in the data block. The transmitting device calculates the value and appends it to the data block; the receiving end makes a similar calculation and compares its results to the added character. If there is a difference, the recipient requests retransmission.

DOD—Department of Defense.

D2—A rating provided by the NCSC for PC security subsystems that corresponds to the features of the C2 level. A computer security subsystem is any hardware, firmware and software which are added to a computer system to enhance the security of the overall system.

DA—Destination address.

DAC—Discretionary access controls.

DAC—Dual attached concentrator.

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.

DARPA—Defense Advanced Research Projects Agency.

DAS—Dual Attachment Station (FDDI, CDDI).

DASS—Distributed authentication security service.

Data—Raw facts and figures that are meaningless by themselves. Data can be expressed in characters, digits, and symbols, which can represent people, things, and events.

Data administration—The function in an organization that plans for, oversees the development of, and monitors the information resource.

Data administration subsystem—Helps manage the overall database environment by providing facilities for backup and recovery, security management, query optimization, concurrency control, and change management.

Data Aggregation—See Part II, 45 CFR 164.501.

Data Classification—Data classification is the assigning a level of sensitivity to data as they are being created, amended, enhanced, stored, or transmitted. The classification of the data should then determine the extent to which the data need to be controlled/secured and is also indicative of its value in terms of its importance to the organization.

Data Communications—The transmission of data between more than one site through the use of public and private communications channels or lines.

Data Condition—A description of the circumstances in which certain data is required. Also see Part II, 45 CFR 162.103.

Data Contamination—A deliberate or accidental process or act that compromises the integrity of the original data.

Data Content—Under HIPAA, this is all the data elements and code sets inherent in a transaction, and not related to the format of the transaction. Also see Part II, 45 CFR 162.103.

Data Content Committee (DCC)—See Designated Data Content Committee.

Data Council—A coordinating body within HHS that has high-level responsibility for overseeing the implementation of the A/S provisions of HIPAA.

Data Definition Language (DDL)—A set of instructions or commands used to define data for the data dictionary. A data definition language (DDL) is used to describe the structure of a database.

Data Dictionary—A document or listing defining all items or processes represented in a data flow diagram or used in a system.

Data Diddling—Changing data with malicious intent before or during input to the system.

Data element—The smallest unit of data accessible to a database management system or a field of data within a file processing system.

Data Encryption Standard (DES)—A private key cryptosystem published by the National Institutes of Standards and Technology (NIST). DES is a symmetric block cipher with a block length of 64 bits and an effective key length of 56 bits. DES has been used commonly for data encryption in the forms of software and hardware implementation.

Data flow analysis—A graphic analysis technique to trace the behavior of program variables as they are initialized, modified, or referenced during program execution.

Data flow diagram—A descriptive modeling tool providing a graphic and logical description of a system.

Data grids—Grids that provide shared data storage. Based on a Catalog where Logical File Names are associated to Physical File Names. .

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

Data Interchange Standards Association (DISA)—A body that provides administrative services to X12 and several other standards-related groups.

Data item—A discrete representation having the properties that define the data element to which it belongs. *See also* data element.

Data link—A serial communications path between nodes or devices without any intermediate switching nodes. Also, the physical two-way connection between such devices.

Data Link Layer (DLL)—A layer with the responsibility of transmitting data reliably across a physical link (cabling, for example) using a networking technology such as Ethernet. The DLL encapsulates data into frames (or cells) before it transmits it. It also enables multiple computer systems to share a single physical medium when used in conjunction with a media access control methodology such as CSMA/CD.

Data Manipulation Language (DML)—A data manipulation language (DML) provides the necessary commands for all database operations, including storing, retrieving, updating, and deleting database records.

Data Mapping—The process of matching one set of data elements or individual code values to their closest equivalents in another set of them. This is sometimes called a cross-walk.

Data mart—Subset of a data warehouse in which only a focused portion of the data warehouse is stored.

Data mining—A methodology used by organizations to better understand their customers, products, markets, or any other phase of the business.

Data Model—A conceptual model of the information needed to support a business function or process.

Data networking switches—Equipment that performs the functions of establishing and releasing connections on a data network.

Data Normalization—In data processing, a process applied to all data in a set that produces a specific statistical property. It is also the process of eliminating duplicate keys within a database. Useful as organizations use databases to evaluate various security data.

Data Objects—Objects or information of potential probative value that are associated with physical items. Data objects may occur in different formats without altering the original information.

Data origin authentication—The corroboration that the entity responsible for the creation of a set of data is the one claimed.

Data owner—See *information owner.*

Data profiling—The use of information about your lifestyle and habits to provide a descriptive profile of your life. At its simplest, data profiling is used by marketing companies to identify you as a possible customer. At its most complex data profiling can be used by security services to identify potential suspects for unlawful activity, or to highlight parts of a person's life where other forms of surveillance may reveal something about their activities. In those states where the European Directive on Data Protection is in force, you have rights of access to any data held about you for the purposes of data processing or profiling. .

Data protection engineering—The methodology and tools used to design and implement data protection mechanisms.

Data Record—An identifiable set of data values treated as a unit, an occurrence of a schema in a database, or collection of atomic data items describing a specific object, event, or tuple (e.g., row of a table).

Data representation—The manner in which data is characterized in a computer system and its peripheral devices.

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.

Data Security—The protection of data from accidental or malicious modification, destruction, or disclosure.

Data segment—A collection of data elements accessible to a database management system; a record in a file processing system.

Data set—A named collection of logically related data items, arranged in a prescribed manner and described by control information to which the programming system has access.

Data warehouse—A collection of integrated subject-oriented databases designed to support the Decision Support function, where each unit of data is relevant to some moment in time. The data warehouse contains atomic data and summarized data.

Database—An integrated aggregation of data usually organized to reflect logical or functional relationships among data elements.

Database Administrator (DBA)—(1) A person who is in charge of defining and managing the contents of a database. (2) The individual in an organization who is responsible for the daily monitoring and maintenance of the databases. The database administrator's function is more closely associated with physical database design than the data administrator's function is.

Database Management System (DBMS)—The software that directs and controls data resources.

Database-based Workflow System—Stores the document in a central location and automatically asks the knowledge workers to access the document when it is their turn to edit the document.

Data-dependent Protection—The protection of data at a level that is commensurate with the sensitivity of the entire file.

Datagram—Logical grouping of information sent as a network layer unit over a transmission medium without prior establishment of a virtual circuit. IP datagrams are the primary information units in the Internet. The terms "cell," "frame," "message," "packet," and "segment" are also used to describe logical information groupings at various layers of the OSI Reference Model and in various technology circles.

Data-Link Control Layer—Layer 2 in the SNA architectural model. Responsible for the transmission of data over a particular physical link. Corresponds roughly to the data-link layer of the OSI model.

Data-Link Layer—Layer 2 of the OSI reference model. Provides reliable transit of data across a physical link. The data-link layer is concerned with physical addressing, network topology, line discipline, error notification, ordered delivery of frames, and flow control. The IEEE divided this layer into two sublayers: the MAC sublayer and the LLC sublayer. Sometimes simply called the link layer. Roughly corresponds to the data-link control layer of the SNA model.

Data-mining Agent—An intelligent agent or application that operates in a data warehouse discovering information.

Data-mining Tool—Software tool used to query information in a data warehouse.

Data-Related Concepts—(1) Clinical or medical code sets identify medical conditions and the procedures, services, equipment, and supplies used to deal with them. Nonclinical, nonmedical, or administrative code sets identify or characterize entities and events in a manner that facilitates an administrative process. HIPAA defines a data element as the smallest unit of named information. In X12 language, that would be a simple data element. But X12 also has composite data elements, which aren't really data elements, but are groups of closely related data elements that can repeat as a group. X12 also has segments, which are also groups of related data elements that tend to occur together, such as street address, city, and state. These segments can sometimes repeat, or one or more segments may be part of a loop that can repeat. For example, you might have a claim loop that occurs once for each claim, and a claim service loop that occurs once for each service included in a claim. An X12 transaction is a collection of such loops, segments, etc. that supports a specific business process, whereas an X12 transmission is a communication session during which one or more X12 transactions is transmitted. (2) Data elements and groups may also be combined into records that make up conventional files, or into the tables or segments used by DBMS. A designated code set is a code set that has been specified within the body of a rule. These are usually medical code sets. Many other code sets are incorporated into the rules by reference to a separate document, such as an implementation guide, that identifies one or more such code sets. These are usually administrative code sets. (3) Electronic data is data that is recorded or transmitted electronically, whereas non-electronic data would be everything else. Special cases would be data transmitted by fax and audio systems, which is, in principle, transmitted electronically, but which lacks the underlying structure usually needed to support automated interpretation of its contents. (4) Encoded data is data represented by some identification or classification scheme, such as a provider identifier or a procedure code. Non-encoded data would be more nearly freeform, such as a name, a street address, or a description. Theoretically, of course, all data, including grunts and smiles, is encoded. (5) For HIPAA purposes, internal data, or internal code sets, are data elements that are fully specified within the HIPAA implementation guides. For X12 transactions, changes to the associated code values and descriptions must be approved via the normal standards development process, and can only be used in the revised version of the standards affected. X12 transactions also use many coding and identification schemes that are maintained by external organizations. For these external code sets, the associated values and descriptions can change at any time and still be usable in any version of the X12 transactions that uses the associated code set. (6) Individually identifiable data is data that can be readily associated with a specific individual. Examples would be a name, a personal identifier, or a full street address. If life were simple, everything else would be non-identifiable data. But even if you remove the obviously identifiable data from a record, other data elements present can also be used to re-identify it. For example, a birth date and a zip code might be sufficient to re-identify half the records in a file. The re-identifiability of data can be limited by omitting, aggregating, or altering such data to the extent that the risk of it being re-identified is acceptable. (7) A specific form of data representation, such as an X12 transaction, will generally include some structural data that is needed to identify and interpret the transaction itself, as well as the business data content that the transaction is designed to transmit. Under HIPAA, when an alternate form of data collection such as a browser is used, such structural or format-related data elements can be ignored as long as the appropriate business data content is used. (8) Structured data is data the meaning of which can be inferred to at least some extent based on its absolute or relative location in a separately defined data structure. This structure could be the blocks on a form, the fields in a record, the relative positions of data elements in an X12 segment, etc. Unstructured data, such as a memo or an image, would lack such clues.

DAU—User data protection data authentication.

DBMS—Database management system.

DCC—See Data Content Committee.

DCE—Data circuit-terminating equipment.

D-Codes—A subset of the HCPCS Level II medical code set with a high-order value of "D" that has been used to identify certain dental procedures. The final HIPAA transactions and code sets rule states that these D-codes will be dropped from the HCPCS, and that CDT codes will be used to identify all dental procedures.

DD— See Data Dictionary.

DDE— See Direct Data Entry.

DDoS Attacks—Distributed denial of service attacks. These are denial-of-service assault from multiple sources. .

DDP—Datagram Delivery Protocol (AppleTalk).

DDR (1)—Dial-on-demand routing.

DDR (2)—Dual data rate RAM.

Dead drop—A method of secret information exchange where the two parties never meet.

Deadlock—A condition that occurs when two users invoke conflicting locks in trying to gain access to a specific record or records.

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

Debugging—The process of correcting static and logical errors detected during coding. With the primary goal of obtaining an executable piece of code, debugging shares certain techniques and strategies with testing but differs in its usual ad hoc application and scope.

DeCC—See Dental Content Committee.

Decentralized computing—An environment in which an organization splits computing power and locates it in functional business areas as well as on the desktops of knowledge workers.

Deceptive trade practices—Misleading or misrepresenting products or services to consumers and customers. In the United States these practices are regulated by the Federal Trade Commission at the federal level and typically by the Attorney General's Office of Consumer Protection at the state level. Microsoft: http://www.microsoft.com/ security/glossary/.

Decipher—The ability to convert, by use of the appropriate key, enciphered text into its equivalent plaintext.

Decipherment—The reversal of a corresponding reversible encipherment.

Decision processing enterprise information portal—Provides knowledge workers with corporate information for making key business decisions.

Decision Superiority—Better decisions arrived at and implemented faster than an opponent can react, or in a noncombat situation, at a tempo that allows the force to shape the situation or react to changes and accomplish its mission.

Decision Support System (DSS)—A computer information system that helps executives and managers formulate policies and plans. This support system enables the users to access information and assess the likely consequences of their decisions through scenario projections.

Declassification—The determination that particular classified information no longer requires protection against unauthorized disclosure in the interest of national security. Such determination shall be by specific action or automatically after the lapse of a requisite period of time or the occurrence of a specified event. If such determination is by specific action, the material shall be so marked with the new designation.

Declassification Event—An event which would eliminate the need for continued classification.

Decoding—Changing a digital signal into analog form or another type of digital signal. The opposite of encoding.

Decontrol—The authorized removal of an assigned administrative control designation.

Decrypt—Synonymous with decipher.

Decrypt/Decipher/Decode—Decryption is the opposite of encryption. It is the transformation of encrypted information back into a legible form. Essentially, decryption is about removing disguise and reclaiming the meaning of information.

Decryption—The conversion through mechanisms or procedures of encrypted data into its original form.

Decryption Key—A piece of information, in a digitized form, used to recover the plaintext from the corresponding ciphertext by decryption.

Dedicated Lines—Private circuits between two or more stations, switches, or subscribers.

Dedicated Mode—The operation of a computer system such that the central computer facility, connected peripheral devices, communications facilities, and all remote terminals are used and controlled exclusively by the users or groups of users for the processing of particular types and categories of information.

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. .

Dedicated server—A microcomputer used exclusively to perform a specific service, such as to process the network operating system.

Deduction—A method of logical reasoning which results in necessarily true statements. As an example, if it is known that every man is mortal and that George is a man, then it can be deduced that George is mortal. Deduction is equivalent to the logical rule of modus ponens.

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. .

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. .

Defense Information Infrastructure (DII)—The complete set of DoD information transfer and processing resources, including information and data storage, manipulation, retrieval, and display. More specifically, the DII is the shared or interconnected system of computers, communications, data, applications, security, people, training, and other support structure, serving the DoD's local and worldwide information needs. It connects DoD mission support, command and control, and intelligence computers and users through voice, data, imagery, video, and multimedia services; and it provides information processing and value-added services to subscribers over the DISN and interconnected Service and Agency networks. Data, information, and user applications software unique to a specific user are not considered part of the DII.

Defense Information Systems Network (DISN)—A subelement of the Defense Information Infrastructure (DII), the DISN is the DoD's consolidated worldwide enterprise level telecommunications infrastructure that provides the end-to-end information transfer network for supporting military operations. It is transparent to its users, facilitates the management of information resources, and is responsive to national security and defense needs under all conditions in the most efficient manner.

Defense-in-depth—The practice of layering defenses to provide added protection. Security is increased by raising the cost to mount the attack. This system places multiple barriers between an attacker and an organization's business critical information resources. This strategy also provides natural areas for the implementation of intrusion-detection technologies.

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.

Degauss—To erase or demagnetize magnetic recording media (usually tapes) by applying a variable, alternating current (AC) field.

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.

Degree (of a relation)—The number of attributes or columns of a relation.

DEL—Delivery and operation, delivery.

Delegated Accrediting Authority (DAA)—Official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. This term is synonymous with designated accrediting authority and designated approval authority.

Delegation—The notation that an object can issue a request to another object in response to a request. The first object therefore delegates the responsibility to the second object. Delegation can be used as an alternative to inheritance.

Delphi—A forecasting method where several knowledgeable individuals make forecasts and a forecast is derived by a trained analyst from a weighted average.

Demand aggregation—Combines purchase requests from multiple buyers into a single large order, which justifies a discount from the business.

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

Demodulation—The reconstruction of an original signal from the modulated signal received at a destination device.

Denial of Service (DOS)—The unauthorized prevention of authorized access to resources or the delaying of time-critical operations.

Denial-of-Service (DoS) attack—The attacker floods a Web site with many electronic message requests for service that it slows down or crashes the network or computer targeted.

Dental Content Committee (DeCC)—An organization hosted by the American Dental Association that maintains the data content specifications for dental billing. The Dental Content Committee has a formal consultative role under HIPAA for all transactions affecting dental healthcare services.

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.

Depth—(1) Penetration layer achieved during or the degree of intensity of an IO attack. (2) The most profound or intense part or stage. The severest or worst part. The degree of richness or intensity.

Derivative Classification—A determination that information is in substance the same as information currently classified, coupled with the designation of the level of classification.

DES—Data Encryption Standard.

Descriptive Attributes—The intrinsic characteristics of an object.

Descriptor—The text defining a code in a code set. Also see Part II, 45 CFR 162.103.

Design—The aspect of the specification process that involves the prior consideration of the implementation. Design is the process that extends and modifies an analysis specification. It accommodates certain qualities including extensibility, reusability, testability, and maintainability. Design also includes the specification of implementation requirements such as user interface and data persistence.

Design and Implementation—A phase of the systems development life cycle in which a set of functional specifications produced during systems analysis is transformed into an operational system for hardware, software, and firmware.

Design Review—The quality assurance process in which all aspects of a system are reviewed publicly.

Designated Accrediting Authority (DAA)—Official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. This term is synonymous with designated approval authority and delegated accrediting authority.

Designated Approving Authority (DAA)—The official who has the authority to decide on accepting the security safeguards prescribed for an AIS or that official who may be responsible for issuing an accreditation statement that records the decision to accept those safeguards.

Designated Code Set— A medical code set or an administrative code set that HHS has designated for use in one or more of the HIPAA standards.

Designated Data Content Committee or Designated DCC— An organization that HHS has designated for oversight of the business data content of one or more of the HIPAA-mandated transaction standards.

Designated Record Set— See Part II, 45 CFR 164.501.

Designated Standard— A standard that HHS has designated for use under the authority provided by HIPAA.

Designated Standard Maintenance Organization (DSMO)— See Part II, 45 CFR 162.103.

Desktop computer—The most popular choice for personal computing needs.

Desktop publishing—The use of computer technology equipped with special hardware, firmware, and software features to produce documents that look equivalent to those printed by a professional print company.

Destruction—Irretrievable loss of data file, or damage to hardware or software.

Detect—To discover threat activity within information systems, such as initial intrusions, during the threat activity or post-activity. Providing prompt awareness and standardized reporting of attacks and other anomalous external or internal system and network activity.

Developer—The organization that develops the IS.

DHCP—Dynamic Host Configuration Protocol.

DHHS—See HHS.

Dial-Up—Access to switched network, usually through a dial or push-button telephone.

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

DICOM—See Digital Imaging and Communications in Medicine.

Dielectric—A nonconducting or insulating substance that resists passage of electric current, allowing electrostatic induction to act across it, as in the insulating medium between the plates of a condenser.

Diffraction—Signal loss as a result of variations in the terrain the signal crosses.

Digimark—a company that creates digital watermarking technology used to authenticate, validate and communicate information within digital and analog media.

Digit—A single numeral representing an arithmetic value.

Digital—A mode of transmission where information is coded in binary form for transmission on the network.

Digital Audio Tape (DAT)—A magnetic tape technology. DAT uses 4-mm cassettes capable of backing up anywhere between 26 and 126 bytes of information.

Digital cash—An electronic representation of cash. Also called e-cash.

Digital Certificates—A certificate identifying a public key to its subscriber, corresponding to a private key held by that subscriber. It is a unique code that typically is used to allow the authenticity and integrity of communication can be verified.

Digital Code Signing—The process of digitally signing computer code so that its integrity remains intact and it cannot be tampered with.

Digital divide—The fact that different peoples, cultures, and areas of the world or within a nation do not have the same access to information and telecommunications technologies.

Digital economy—Marked by the electronic movement of all types of information, not limited to numbers, words, graphs, and photos but also including physiological information such as voice recognition and synthesization, biometrics (a person's retina scan and breath, for example), and 3-D holograms.

Digital fingerprint—A characteristic of a data item, such as a cryptographic checkvalue or the result of performing a one-way hash function on the data, that is sufficiently peculiar to the data item that it is computationally infeasible to find another data item that possesses the same characteristics.

Digital Imaging and Communications in Medicine (DICOM)—A standard for communicating images, such as x-rays, in a digitized form. This standard could become part of the HIPAA claim attachments standards.

Digital modem—A piece of equipment that joins a digital phone line to a piece of communication equipment, which may be a phone or a PC. Such equipment allows testing, condition, timing, interfacing, etc. But it does not do what a modem does: namely convert digital signals from machines into analog signals which can be carried on analog phone lines. The term digital modem, thus, is somewhat of a misnomer.

Digital PABX—An automatic switching system. No operator is needed to complete the call. In the original PBX system operators were sometimes needed to complete the calls. Also called Private Automatic Branch Exchange.

Digital Rights Management (DRM)—Focuses on security and encryption to prevent unauthorized copying limit distribution to only those who pay. This is considered first-generation DRM. Second-generation DRM covers: description, identification, trading, protection, monitoring and tracking of all forms of rights usages over both tangible and intangible assets including management of rights holders' relationships. It is important to note that DRM manages all rights, not just those involving digital content. Additionally, it is important to note that DRM is the "digital management of rights" and not the "management of digital rights". That is, DRM manages *all* rights, not only the rights applicable to permissions over digital content.

Digital signature—The act of electronically affixing an encrypted message digest to a computer file or message in which the originator is then authenticated to the recipient.

Digital Signature Standard (DSS)—The National Security Administration's standard for verifying an electronic message.

Digital Subscriber Line (DSL)—A technology that dramatically increases the digital capacity of ordinary telephone lines (the local loops) into the home or office. DSL speeds are tied to the distance between the customer and the telephone company's central office.

Digitize—Converting an analog or continuous signal into a series of 1s and 0s, i.e., into a digital format.

DII—Defense information infrastructure.

DIMM—Dual Inline Memory Module.

Diode—Devices that conduct electricity in one direction only. They are sometimes referred to as PN (positive-negative) devices because they are made of a single semiconductive crystal with a positive terminal and a negative terminal.

Direct Access—The method of reading and writing specific records without having to process all preceding records in a file.

Direct Access Storage Device (DASD)—A data storage unit on which data can be accessed directly without having to progress through a serial file such as a magnetic tape file. A disk unit is a direct access storage device.

Direct current—A flow of electricity always in the same direction.

Direct Data Entry (DDE)—Under HIPAA, this is the direct entry of data that is immediately transmitted into a health plan's computer. Also see Part II, 45 CFR 162.103.

Direct organization—A method of file organization under which records are located on the basis of their keys and associated addresses on the storage media.

Direct Treatment Relationship—See Part II, 45 CFR 164.501.

Direction of Arrival (DoA)—The electromagnetic waves arrive at the directional antenna and are received more readily from one direction than from another. The antenna needs to be aligned with the direction of arrival.

Directory—A table specifying the relationships between items of data. Sometimes a table (index) giving the addresses of data.

Directory engine search—Organizes listings of Web sites into hierarchical lists.

Directory service—A service provided on a computer network that allows one to look up addresses (and perhaps other information such as public key certificates) based upon user-names.

DISA—See the Data Interchange Standards Association.

Disaster Notification Fees—The fee a recovery site vendor usually charges when the customer notifies them that a disaster has occurred and the recovery site is required. The fee is implemented to discourage false disaster notifications.

Disaster recovery cost curve—Charts (1) the cost to the organization due to the unavailability of information and technology, and (2) the cost to the organization of recovering from a disaster over time.

Disaster recovery plan—A detailed process for recovering information or an IT system in the event of a catastrophic disaster such as a fire or flood.

Disc Mirroring—This is the practice of duplicating data in separate volumes on two hard disks to make storage more fault-tolerant. Mirroring provides data protection in the case of disk failure, because data is constantly updated to both disks.

Disclosure—The release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information. (See Use, in contrast.).

Disclosure History—Under HIPAA, this is a list of any entities that have received personally identifiable healthcare information for uses unrelated to treatment and payment.

Discrepancy Reports—A listing of items that have violated some detective control and require further investigation.

Discrete Cosine Transform (DCT)—used in JPEG compression, the discrete cosine transform helps separate the image into parts of differing importance based on the image's visual quality; this allows for large compression ratios. The DCT function transforms data from a spatial domain to a frequency domain.

Discretionary Access Control (DAC)—A means of restricting access to objects based on the identity of subjects and groups to which they belong. The controls are discretionary in the sense that a subject with certain access permission is capable of passing that permission on to another subject.

Disintermediation—The use of the Internet as a delivery vehicle whereby intermediate players in a distribution channel can be bypassed.

Disk address—The positioned location of a data record on magnetic disk storage.

Disk Duplexing—This refers to the use of two controllers to drive a disk subsystem. Should one of the controllers fail, the other is still available for disk I/O. Software applications can take advantage of both controllers to simultaneously read and write to different drives.

Disk Mirroring—Disk mirroring protects data against hardware failure. In its simplest form, a two-disk subsystem would be attached to a host controller. One disk serves as the mirror image of the other. When data is written to it, it is also written to the other disk. Both disks will contain exactly the same information. If one fails, the other can supply the user data without problem.

Disk Operating System (DOS)—Software that controls the execution of programs and may provide system services as resource allocation.

Disk optimization software—Utility software that organizes information on the hard disk in the most efficient way.

Diskette—A flexible disk storage medium most often used with microcomputers; also called a floppy disk.

Distinguishing identifier—Data that unambiguously distinguishes an entity in the authentication process. Such an identifier shall be unambiguous at least within a security domain.

Distortion—An undesired change in an image or signal. A change in the shape of an image resulting from imperfections in an optical system, such as a lens.

Distributed application—A set of information processing resources distributed over one or more open systems which provides a well-defined set of functionality to (human) users, to assist a given (office) task.

Distributed Component Object Model (DCOM)—A protocol that enables software components to communicate directly over a network. Developed by Microsoft and previously called “Network OLE,” DCOM is designed for use across multiple network transports including Internet Protocols such as HTTP.

Distributed Computing—The distribution of processes among computing components that are within the same computer or different computers on a shared network.

Distributed Computing Environment (DCE)—An architecture of standard programming interfaces, conventions, and server functionalities (e.g., naming, distributed file system, remote procedure call) for distributing applications transparently across networks of heterogeneous computers. Promoted and controlled by the Open Software Foundation (OSP), a consortium led by Hewlett-Packard, Digital Equipment Corp, and IBM.

Distributed Database—A database management system with the ability to effectively manage data that is distributed across multiple computers on a network.

Distributed Denial-of-Service (DDoS) Attack—Multiple computers flooding a Web site with so many requests for service that it slows down or crashes.

Distributed Environment—A set of related data processing systems in which each system has its own capacity to operate autonomously but has some applications that are executed at multiple sites. Some of the systems may be connected with teleprocessing links into a network with each system serving as a node.

Distributed System—A multi-work station, or terminal system where more than one workstation shares common system resources. The work stations are connected to the control unit/data storage element through communication lines.

Dithering—Creating the illusion of new colors and shades by varying the pattern of dots in an image. Dithering is also the process of converting an image with a certain bit depth to one with a lower bit depth.

DITSCAP—Department of Defense Information Technology 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.

DIX—Digital-Intel-Xerox.

DLC—Data Link Control.

DLCI—Data Link Connection Identifier (Frame Relay).

DME— Durable Medical Equipment.

DMEPOS— Durable Medical Equipment, Prosthetics, Orthotics, and Supplies.

DMERC— See Medicare Durable Medical Equipment Regional Carrier.

DMZ—Commonly, it is the network segment between the Internet and a private network. It allows access to services from the Internet and the internal private network, while denying access from the Internet directly to the private network.

DNA SCP—Digital Network Architecture Session Control Protocol (DECnet).

DNIC—Data Network Identification Code (X.25).

DNS (Domain Name System, Service or Server)—A hierarchical database that is distributed across the Internet and allows names to be resolved to IP addresses and vice versa to locate services such as Web sites and email. An Internet service that translates domain names into IP addresses.).

Document—Any recorded information regardless of its physical form or characteristics, including, without limitation, written or printed material; data processing cards and tapes; maps; charts; paintings; drawings; engravings; sketches; working notes and papers; reproductions of such things by any means or process; and sound, voice, or electronic recordings in any form.

Documentation—The written narrative of the development, workings, and operation of a program or system.

DoD Information Technology Security Certification and Accreditation Process (DITSCAP)—The standard DoD process for identifying information security requirements, providing security solutions, and managing IS security activities.

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—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.

Domain Dimension—The dimension dealing with the structural aspects of the system involving broad, static patterns of internal behavior.

Domain Name—The name used to identify an Internet host.

Domain Name Server—See DNS.

Domain name system (DNS)—The distributed name and address mechanism used in the Internet.

Domain of Interpretation (DOI)—The DOI defines payload formats, the situation, exchange types, and naming conventions for certain information such as security policies, or cryptographic algorithms. It is also used to interpret the ISAKMP payloads.

DoS—(1) Short for *denial-of-service attack,* a type of attack on a network that is designed to bring the network to its knees by flooding it with useless traffic. For all known DoS attacks, there are software fixes that system administrators can install to limit the damage caused by the attacks. (2) In general, any malicious action that denies availability of a system to users.

Downgrading—The determination that particular classified information requires a lesser degree of protection or no protection against unauthorized disclosure than currently provided. Such determination shall be by specific action or automatically after lapse of the requisite period of time or the occurrence of a specified event. If such determination is by specific action, the material shall be so marked with the new designation.

Downlink frequencies—Frequencies used in the transmission link reaching from a satellite to the ground.

Downtime—A period of time in which the computer is not available for operation.

DPT—Tests, depth.

DQDB—Distributed Queue Dual Bus (SMDS).

DR—Designated router.

Draft Standard for Trial Use (DSTU)—An archaic term for any X12 standard that has been approved since the most recent release of X12 American National Standards. The current equivalent term is "X12 standard.".

DRAM—Dynamic random access memory.

DRG—Diagnosis Related Group.

DRP—Disaster recovery plan.

DS-0—Digital Signal, level 0. A DS-0 is a voice-grade channel of 64 kbps.

DS-1—Digital Signal Level 1 (1.544 Mb).

DS-3—Digital Signal Level 3 (45 Mb).

DSA—Digital Signature Algorithm.

DSAP—Destination Service Access Point (LLC).

DSE—Data switching equipment.

DSL—Digital Subscriber Line.

DSMO— See Designated Standard Maintenance Organization.

DSR—Data set ready.

DSS—Digital signature standard; see FIPS PUB 186.165.

DSS (1)—Digital Subscriber Signaling System 1.

DSS (2)—Digital Signature Standard.

DSS shell—A set of programs that can be used for constructing a decision support system.

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

DSTU— See Draft Standard for Trial Use.

DSU—Data service unit.

DTE—Domain and type enforcement.

DTE—Data terminal equipment.

DTR—Data terminal ready.

DUAL—Diffused update algorithm (EIGRP).

Dual Control—A procedure that uses to or more entities (usually persons) operating in concert to protect a system resources, such that no single entity acting alone can access that resource.

Dual Tone Multifrequency (DTMF)—A term describing push button or touch-tone dialing. When you push a button, it makes a tone that is actually a combination of two tones, one high frequency and one low frequency.

Due care—Managers and their organizations have a duty to provide for information security to ensure that the type of control, the cost of control, and the deployment of control are appropriate for the system being managed. .

Dumb Terminal—A device used to interact directly with the end user where all data is processed on a remote computer. A dumb terminal only gathers and displays data; it has no processing capability.

Dump—The contents of a file or memory that are output as listings. These listing can be formatted.

Duplex—Communications systems or equipment that can simultaneously carry information in both directions between two points. Also used to describe redundant equipment configurations (e.g., duplexed processors).

DVS—Lifecycle support, development security.

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.

Dynamic binding—The responsibility for executing an action on an object resides within the object itself. The same message can elicit a different response depending upon the receiver.

Dynamic Dimension—The dimension concerned with the nonstatic, process related properties of the system.

Dynamic Host Configuration Protocol (DHCP)—DHCP is an industry standard protocol used to dynamically assign IP addresses to network devices.

Dynamic processing—The technique of swapping jobs in and out of computer memory. This technique can be controlled by the assignment priority and the number of time slices allocated to each job.

Dynamically Phased Array (PA)—Type of radio antenna used in certain satellite and wireless communications. This small flat antenna mounts on the side of a building or on a rooftop. It has an array of chip-based radio receivers, which lock in on the target transmission frequency on a dynamic basis. Also called a "pizza box antenna.".

EAL—Evaluation assurance level.

EAP—Extensible Authentication Protocol.

Early Token Release—Technique used in Token Ring networks that allows a station to release a new token onto the ring immediately after transmitting, instead of waiting for the first frame to return. This feature can increase the total bandwidth on the ring. *See also* Token Ring.

Earth Stations—Ground terminals that use antennas and other related electronic equipment designed to transmit, receive, and process satellite communications.

Ease—Amount of time and skill level required to either penetrate or restore function. Measures the degree of difficulty.

Eavesdropping—The unauthorized interception of information-bearing emanations through methods other than wiretapping.

EBCDIC—Extended Binary Encoded Decimal Interchange Code.

EBGP—Exterior Border Gateway Protocol.

ebXML—A set of technical specifications for business documents built around XML designed to permit enterprises of any size and in any geographical location to conduct business over the Internet.

EC— See *electronic commerce.*

ECC—Elliptic curve cryptography.

Echo—The display of characters on a terminal output device as they are entered into the system.

Echo hiding—Relies on limitations in the human auditory system by embedding data in a cover audio signal. Using changes in delay and relative amplitude; two types of echos are created which allows for the encoding of one's and zeros.

Ecological Dimension—The dimension dealing with the interface properties of a system; inflow and outflow of forces in a system.

Economy—Scaleable system packages ease the application of economy. Space, weight, or time constraints limit the quantity or capability of systems that can be deployed. Information requirements must be satisfied by consolidating similar functional facilities, integrating commercial systems into tactical information works, or accessing to a different information system.

EDI—Electronic Data Interchange (Computer to computer transactions).

EDI Translator— A software tool for accepting an EDI transmission and converting the data into another format, or for converting a non-EDI data file into an EDI format for transmission.

EDIFACT— See United Nations Rules for Electronic Data Interchange for Administration, Commerce, and Transport (UN/EDIFACT).

Edit—The process of inspecting a data field or element to verify the correctness of its content.

EDP auditor—A professional whose responsibility is to certify the validity, reliability, and integrity of all aspects of the computer information system environment of an organization, a.k.a. IS auditor, CIS auditor, or IT auditor.

Education—IT security education focuses on developing the ability and vision to perform complex, multidisciplinary activities and the skills needed to further the IT security profession. Education activities include research and development to keep pace with changing technologies and threats.

EEPROM—Electrically erasable programmable read-only memory.

Effective Date—Under HIPAA, this is the date that a final rule is effective, which is usually 60 days after it is published in the Federal Register.

Effectiveness—Efficiency, potency, or capability of an act in producing a desired (or undesired) result. The power of the protection or the attack.

Efficiency—Capability, competency, or productivity. The efficiency of an act is a measure of the work required to achieve a desired result.

EFT—See Electronic Funds Transfer.

E-government—The application of E-commerce technologies in government agencies.

EGP—Exterior Gateway Protocol.

EHNAC—See the Electronic Healthcare Network Accreditation Commission.

EIA—Electronic Industries Association.

EIGRP—Enhanced Interior Gateway Routing Protocol.

EIN—Employer Identification Number.

Electromagnetic Emanations—Signals transmitted as radiation through the air or conductors.

Electromagnetic Interference (EMI)—Electromagnetic waves emitted by a device.

Electron—A light, subatomic particle that carries a negative charge.

Electronic Attack (EA)—Use of EM or Directed Energy to attack personnel, facilities or equipment to destroy/degrade combat capability.

Electronic Bill Presentation and Payment (EBPP)—A system that sends people their bills over the Internet and gives them an easy way to pay.

Electronic bulletin board—An application program that lets users contribute messages via e-mail that can be routed or shared with users.

Electronic business XML—See ebXML.

Electronic catalog—Designed to present products to customers via the Internet.

Electronic Code Book (ECB)—A basic encryption method that provides privacy but not authentication.

Electronic commerce—A broad concept that covers any trade or commercial transaction that is effected via electronic means; this would include such means as facsimile, telex, EDI, Internet, and the telephone. For the purpose of this book the term is limited to those commercial transactions involving computer to computer communications whether utilizing an open or closed network.

Electronic Communications Privacy Act of 1986 PL 99-508 (ECPA)—Electronic Communications Privacy Act of 1986; extends the Privacy Act of 1974 to all forms of electronic communication, including email.

Electronic Data Interchange (EDI)—A process whereby such specially formatted documents as an invoice can be transmitted from one organization to another. A system allowing for inter-corporate commerce by the automated electronic exchange of structured business information.

Electronic Data Vaulting—Electronic vaulting protects information from loss by providing automatic and transparent backup of valuable data over high-speed phone lines to a secure facility.

Electronic document file—A magnetic storage area that contains electronic images of papers and other communications documents.

Electronic Frontier Foundation—A foundation established to address social and legal issues arising from the impact on society of the increasingly pervasive use of computers as the means of communication and information distribution.

Electronic Funds Transfer (EFT)—The process of moving money between accounts via computer.

Electronic Healthcare Network Accreditation Commission (EHNAC)—An organization that tests transactions for consistency with the HIPAA requirements, and that accredits healthcare clearinghouses.

Electronic job market—Consists of employers using the Internet to advertise for and screen potential employees.

Electronic Journal—A computerized log file summarizing, in chronological sequence, the processing activities and events performed by a system. The log file is usually maintained on magnetic storage media.

Electronic mail (e-mail)—Formal or informal communications electronically transmitted or delivered.

Electronic Media Claims (EMC)—This term usually refers to a flat file format used to transmit or transport claims, such as the 192-byte UB-92 Institutional EMC format and the 320-byte Professional EMC NSF.

Electronic office—An office that relies on word processing, computer systems, and communications technologies to support its operations.

Electronic portfolio—Collection of Web documents used to support a stated purpose such as writing skills.

Electronic Protect (EP)—Actions to protect personnel, facilities and equipment from enemy/friendly EW that degrade or destroy own-force combat capability.

Electronic Remittance Advice (ERA)—Any of several electronic formats for explaining the payments of healthcare claims.

Electronic Signature—Any technique designed to provide the electronic equivalent of a handwritten signature to demonstrate the origin and integrity of specific data. Digital signatures are an example of electronic signatures.

Electronic Warfare (EW)—Action involving the use of electromagnetic (EM) and directed energy to control the EM spectrum or to attack the enemy.

Electronic Warfare Support (ES)—That division of EW involving actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition. Thus, electronic warfare support provides information required for immediate decisions involving EW operations and other tactical actions such as threat avoidance, targeting and homing. ES data can be used to produce signals intelligence .

Element management functions—A set of functions for management of network elements on an individual basis. These are basically the same functions as those supported by the corresponding local terminals.

Element manager—Provides a package of end-user functions for management of a set of closely related types of network elements. .

E-mail software (electronic mail software)—Enables people to electronically communicate with other people by sending and receiving e-mail.

Emanation Security—The protection that results from all measures designed to deny unauthorized persons access to valuable information that might be derived from interception and analysis of compromising emanations.

Embedded message—In steganography, it is the hidden message that is to be put into the cover medium.

Embedding—To cause to be an integral part of a surrounding whole. In steganography and watermarking, embedding refers to the process of inserting the hidden message into the cover medium.

EMC—Electromagnetic conductance.

EMC—See Electronic Media Claims.

EMF—Electromagnetic field.

EMI—Electromagnetic interference.

Emission Security (EMSEC)—The protection resulting from all measures taken to deny unauthorized persons information of value that might be derived from intercept and from an analysis of compromising emanations from systems.

EMP—Electromagnetic pulse.

EMR—Electronic Medical Record.

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

Encapsulated subsystem—A collection of procedures and data objects that is protected in a domain of its own so that the internal structure of a data object is accessible only to the procedures of the encapsulated subsystem and that those procedures may be called only at designated domain entry points. Encapsulated subsystem, protected subsystem and protected mechanisms of the TCB are terms that may be used interchangeably.

Encapsulation—The technique used by layered protocols in which a layer adds header information to the protocol data unit (PDI) from the layer above.

Encipher—The process of converting plaintext into unintelligible form by means of a cipher system.

Encipherment—The cryptographic transformation of data (see cryptography) to produce ciphertext.

Enclave—An environment that is under the control of a single authority and has a homogeneous security policy, including personnel and physical security. Local and remote elements that access resources within an enclave must satisfy the policy of the enclave. Enclaves can be specific to an organization or a mission and may also contain multiple networks. They may be logical, such as an operational area network (OAN) or be based on physical location and proximity.

Encoding—The process of converting data into code or analog voice into a digital signal.

Encrypt—To scramble information so that only someone knowing the appropriate secret can obtain the original information (through decryption).

Encrypt/Encipher/Encode—Encryption is the transformation of information into a form that is impossible to read unless you have a specific piece of information, which is usually referred to as the “key.” The purpose is to keep information private from those who are not intended to have access to it. To encrypt is essentially about making information confusing and hiding the meaning of it.

Encrypted Text—Data which is encoded into an unclassified form using a nationally accepted form of encoding.

Encryption—The use of algorithms to encode data in order to render a message or other file readable only for the intended recipient.

Encryption Algorithm—A set of mathematically expressed rules for encoding information, thereby rendering it unintelligible to those who do not have the algorithm decoding key.

Encryption Key—A special mathematical code that allows encryption hardware/software to encode and then decipher an encrypted message.

End Entity—An End Entity can be considered as an end-user, a device such as a router or a server, a process, or anything that can be identified in the subject name of a public key certificate. End Entities can also be thought of as consumers of the PKI-related services.

End System—An OSI system that contains application processes capable of communication through all seven layers of OSI protocols. Equivalent to Internet host.

Endorsed Cryptographic Products List—A list of products that provide electronic cryptographic coding (encrypting) and decoding (decrypting), and which have been endorsed for use for classified or sensitive unclassified U.S. government or government-derived information during its transmission.

Endorsed TEMPEST Products List—A list of commercially developed and commercially produced TEMPEST telecommunications equipment that NSA has endorsed, under the auspices of the NSA Endorsed TEMPEST Products Program, for use by government entities and their contractors to process classified U.S. government information.

End-to-end encipherment—Encipherment of data within or at the source end system, with the corresponding decipherment occurring only within or at the destination end system.

End-to-end encryption—The encryption of information at the point of origin within the communications network and postponing of decryption to the final destination point.

Enrollment—The initial process of collecting biometric data from a user and then storing it in a template for later comparison.

Enterprise Application Integration (EAI)—The process of developing an IT infrastructure that enables employees to implement new or changing business processes.

Enterprise Application Integration middleware (EAI middleware)—Allows organizations to develop different levels of integration from the information level to the business process level.

Enterprise Information Portal (EIP)—Allows knowledge workers to access company information via a Web interface.

Enterprise Resource Planning (ERP)—The method of getting and keeping an overview of every part of the business, so that production and selling of goods and services will be coordinated to contribute to the company's goals.

Enterprise Root—A certificate authority (CA) that grants itself a certificate and creates a subordinate CAs. The root CA gives the subordinate CAs their certificates, but the subordinate CAs can grant certificates to users.

Enterprise software—A suite of software that includes (1) a set of common business applications; (2) tools for modeling how the organization works; and (3) development tools for building applications unique to the organization.

Entity—Either a subject (an active element that operates on information or the system state) or an object (a passive element that contains or receives information).

Entity barrier —A product or service feature that customers have come to expect from companies.

Entity class—A concept — typically people, places, or things — about which information can be stored and then identified with a unique key called the primary key.

Entity-Relationship (ER) diagram —A graphic method of representing entity classes and their relationships.

Entrapment—The deliberate planting of apparent flows in a system to invite penetrations.

ENV—(1) protection profile evaluation, security environment. (2) security target evaluation, security environment.

Environment (System)—The aggregate of procedures, conditions, and objects that affects the development, operation, and maintenance of a system. Note: Environment is often used with qualifiers such as computing environment, application environment, or threat environment, which limit the scope being considered.

EOB—Explanation of Benefits.

EOMB—Explanation of Medicare Benefits, Explanation of Medicaid Benefits, or Explanation of Member Benefits.

EOT—End of transmission.

EPROM—Erasable programmable read-only memory.

EPSDT—Early and Periodic Screening, Diagnosis, and Treatment.

ERA—See Electronic Remittance Advice.

Erasable Programmable Read-Only Memory (EPEOM)—A memory chip that can have its circuit logic erased and reprogrammed.

ERISA— The Employee Retirement Income Security Act of 1974.

ERP—Emergency response plan.

Error—A discrepancy between actual values or conditions and those expected.

Error—The difference between a computed, observed, or measured value or condition and the true, specified, or theoretically correct value or condition.

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.

Error Rate—A measure of the quality of circuits or equipment. The ratio of erroneously transmitted information to the total sent (generally computed per million characters sent).

ESF—Extended Super Framing (T1/E1).

ESP—Encapsulated Security Payload protocol.

Espionage—The practice or employment of spies; the practice of watching the words and conduct of others, to make discoveries, as spies or secret emissaries; secret watching. This category of computer crime includes international spies and their contractors who steal secrets from defense, academic, and laboratory research facility computer systems. It includes criminals who steal information and intelligence from law enforcement computers, and industrial espionage agents who operate for competitive companies or for foreign governments who are willing to pay for the information. What has generally been known as industrial espionage is now being called competitive intelligence. A lot of information can be gained through “open source” collection and analysis without ever having to break into a competitor’s computer. This information gathering is also competitive intelligence, although it is not as ethically questionable as other techniques.

ET—Exchange termination.

E-tailor—An Internet retail site.

ETC—User data protection export to outside TSF control.

Ethernet—A LAN technology that is in wide use today utilizing CSMA/CD (Carrier Sense Multiple Access/Collision Detection) to control access to the physical medium (usually a category 5 Ethernet cable). Normal throughput speeds for Ethernet are 10 Mbps, 100 Mbps, and 1 Gbps.

Ethernet card—The most common type of network interface card.

Ethical (white-hat) hacker—A computer security professional who is hired by a company to break into its computer system.

Ethics—The principles and standards that guide people’s behavior towards others.

ETSI—European Telecommunication Standards Institute.

Evaluated Products List (EPL)—A list of equipments, hardware, software, and firmware that have been evaluated against, and found to be technically compliant, at a particular level of trust, with the DoD TCSEC by the NCSC. The EPL is included in the National Security Agency Information Systems Security Products and Services Catalogue, which is available through the Government Printing Office.

Evaluation—The inspection and testing of specific hardware and software products against accepted Information Assurance/Information Security standards.

Evaluation assurance level—One of seven levels defined by the Common Criteria that represent the degree of confidence that specified functional security requirements have been met by a commercial product.

Evaluation Criteria—See IT Security Evaluation Criteria.

Evaluation Methodology—See IT Security Evaluation Methodology.

Event—A trigger for an activity.

Evolution checking—Testing to ensure the completeness and consistency of a software product at different levels of specification when that product is a refinement or elaboration of another.

Evolutionary Program Strategies—Generally characterized by design, development, and deployment of a preliminary capability that includes provisions for the evolutionary addition of future functionality and changes, as requirements are further defined.

Exception Report—A manager report that highlights abnormal business conditions. Usually, such reports prompt management action or inquiry.

Exchange authentication information—Information exchanged between a claimant and a verifier during the process of authenticating a principal.

Exchange Type—Exchange type defines the number of messages in an ISAKMP exchange and the ordering of the used payload types for each of these messages. Through this arrangement of messages and payloads security services are provided by the exchange type.

Executive Information System (EIS)—A very interactive IT system that allows the user to first view highly summarized information and then choose how to see greater detail, which may be an alert to potential problems or opportunities.

Expand—To increase in extent, number, volume, or scope.

Expandability—Refers to how easy it is to add features or functions to a system.

Expansion bus—Moves information from the CPU and RAM to all other hardware devices such as a microphone or printer.

Expansion card—A circuit board that is inserted into an expansion slot.

Expansion slot—A long skinny pocket on the motherboard into which an expansion card can be inserted.

Expert System—The application of computer-based artificial intelligence in areas of specialized knowledge.

Explanation module—The part of an expert system where the "why" information, supplied by the domain expert, is stored to be accessed by knowledge workers who want to know why the expert systems asked a question or reached a conclusion.

Exposure—The potential loss to an area due to the occurrence of an adverse event.

Extended Binary-Coded Decimal Interchange Code (EBCDIC)—A data representation and code system based on the use of an 8-bit byte.

Extended SuperFrame—A new version of the SuperFrame that allows for more frames to be grouped together. In a T1 circuit, each of the 24 DS0 channels are sampled every 125 microseconds and 8 bits are taken from each. If you multiply the 8 bits by the 24 channels, you get 192-bits in a chain, and then add one bit for timing, you get 193 total bits in one frame. Twelve frames comprise the SuperFrame. For the Extended SuperFrame, we double the number of frames, making the total 24.

Extensibility—A property of software such that new kinds of object or functionality can be added to it with little or no effect to the existing system.

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.

Extensible Markup Language (XML)—Designed to enable the use of SGML on the World Wide Web, XML is a regular markup language that defines what you can do (or what you have done) in the way of describing information for a fixed class of documents (like HTML). XML goes beyond this and allows you to define your own customized markup language. It can do this because it is an application profile of SGML. XML is a metalanguage, a language for describing languages.

External Certificate Authority—An agent that is trusted and authorized to issue certificates to approved vendors and contractors for the purpose of enabling secure interoperability with DoD entities. Operating requirements for ECAs must be approved by the DoD CIO, in coordination with the DoD Comptroller and the DoD General Counsel.

External information—Describes the environment surrounding the organization.

Extraction engine—Smart software with a vocabulary of job-related skills that allows it to recognize and catalog terms in a scannable resume.

Extranet—An intranet that is restricted to an organization and certain outsiders, such as customers and suppliers.

Facsimile (fax)—A technology used to send document images over telecommunications lines.

Fading—Signal disruption caused by multipath signals and heavy rains.

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. See *degraded-mode operation.*

Fail Safe—The automatic termination and protection of programs or other processing operations when a hardware, software, or firmware failure is detected in a computer system.

Fail safe/secure—(1) A design wherein the component/system, should it fail, will fail to a safe/secure condition. (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. .

Fail Soft—The selective termination of nonessential processing affected by a hardware, software, or firmware failure in a computer system.

Failure—Failing to or inability of a system, entity, or component to perform its required function, 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. .

Failure access—Unauthorized and usually inadvertent access to data resulting from a hardware, software, or firmware failure in the computer system.

Failure control—The methodology used to detect and provide fail-safe or fail-soft recovery from hardware, software, or firmware failure in a computer system.

Failure minimization—Actions designed or programmed to reduce failure possibilities to the lowest rates possible. .

Fair Credit Reporting Act (P.L. 91-508)—A federal law that gives individuals the right of access to credit information pertaining to them and the right to challenge such information.

Fair Use Doctrine—Allows the use of copyrighted material in certain situations.

Fallback Procedures—Predefined operations (manual or automatic) invoked when a fault or failure is detected in a system.

Fall-through Logic—Predicting which way a program will branch when an option is presented. It is an optimized code based on a branch prediction.

False Acceptance Rate (FAR)—The percentage of imposters incorrectly matched to a valid user's biometric. False rejection rate (FRR) is the percentage of incorrectly rejected valid users.

FAQ(s)—Frequently Asked Questions.

Fast Ethernet—Any of a number of 100-Mbps Ethernet specifications. Fast Ethernet offers a speed increase ten times that of the 10BaseT Ethernet specification, while preserving such qualities as frame format, MAC mechanisms, and MTU. Such similarities allow the use of existing 10BaseT applications and network management tools on Fast Ethernet networks. Based on an extension to the IEEE 802.3 specification. *Compare with* Ethernet.

FAU—Security audit functional class.

Fault—(1) A defect that results in an incorrect step, process, data value, or mode/state. (2) A weakness of the system that allows circumventing protective controls.

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.

FBI—Federal Bureau of Investigation.

FC—Frame Control (Token Ring).

FCC—Federal Communications Commission.

FCO—Communication functional class.

FCPA—Foreign Corrupt Practices Act.

FCS—Frame check sequence.

FCS—Cryptographic support functional class.

FD—Feasible Distance (EIGRP).

FDA— Food and Drug Administration.

FDD—Floppy Disk Drive.

FDDI—Fiber Distributed Data Interface. This is a Token Ring type of technology that utilizes encoded light pulses transmitted via fiber optic cabling for communications between computer systems. It supports a data rate of 100 Mbps and is more likely to be used as a LAN backbone between servers. It has redundancy built in so that if a host on the network fails, there is an alternate path for the light signals to take to keep the network up.

FDM—Frequency division multiplexing.

FDP—User data protection functional class.

Feasibility study—An investigation of the legal, political, social, operational, technical, economic, and psychological effects of developing and implementing a system.

Feature analysis—The step of ASR in which the system captures the users' words as spoken into a microphone, eliminates any background noise, and converts the digital signals of speech into phonemes (syllables).

Feature creep—Occurs when developers add extra features that were not part of the initial requirements.

FECN—Forward explicit congestion notification.

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

Federal Computer Fraud Act—The Counterfeit Access Device and Computer Fraud and Abuse Act of 1986 outlaws unauthorized access to the federal government's computers and financial databases as protected under the Right to Financial Privacy Act of 1978 and the Fair Credit Reporting Act of 1971. This Act is an amendation of the 1984 Federal Computer Fraud Act.

Feistal Network—A Feistal network generates blocks of keystream from blocks of the message itself, through multiple rounds of groups of permutations and substitutions, each dependent on transformations of a key.

FEP—Front-end processor.

FERPA—Family Educational Rights and Privacy Act.

Fetch Protection—A system-provided restriction to prevent a program from accessing data in another user's segment of storage.

FFIEC—Federal Financial Institutions Examination Council.

FFS—Fee-for-Service.

FI—See Medicare Part A Fiscal Intermediary.

FIA—Identification and authentication functional class.

Fiber Distributed Data Interface (FDDI)—LAN standard, defined by ANSI X3T9.5, specifying a 100-Mbps token-passing network using fiberoptic cable, with transmission distances of up to 2 km. FDDI uses a dual-ring architecture to provide redundancy.

Fiber-optic—A strand of very pure, very clear glass that can carry more information longer distances.

FIC—Federal Interest Computer.

Fiche—A sheet of photographic film containing multiple microimages; a form of computer output microfilm.

Fidelity—Accuracy, exact correspondence to truth or fact, the degree to which a system or information is distortion-free.

Field—A basic unit of data, usually part of a record that is located on an input, storage, or output microfilm.

Field Definition Record (FDR)—A record of field definition. A list of the attributes that define the type of information that can be entered into a data field.

FIFO—First in, first out.

File—A basic unit of data records organized on a storage medium for convenient location, access, and updating.

File creation—The building of master or transaction files.

File format dependence—A factor in determining the robustness of a piece of stegoed media. Coverting an image from on format to another will usually render the embedded message unrecoverable.

File inquiry—The selection of records from files and immediate display of their contents on a terminal output device.

File maintenance—The changing of master file by changing the contents of existing records, adding new records, or deleting old records.

File protection—The aggregate of all processes and procedures established in a computer system and designed to inhibit unauthorized access, contamination, or elimination of a file.

File transfer—The process of copying a file from one computer to another over a network.

File Transfer Protocol (FTP)—The Internet protocol (and program) used to transfer files between hosts.

File updating—The posting of transaction data to master files or maintenance of master files through record additions, changes, or deletions.

Filter—A process or device that screens incoming information for definite characteristics and allows a subset of that information to pass through.

Financial cybermediaries—Internet-based companies that make it easy for one person to pay another over the Internet.

Financial EDI (FEDI)—The use of EDI for payments.

Finger—A program (and a protocol) that displays information about a particular user, or all users, logged on a local system or on a remote system. It typically shows full-time name, last login time, idle time, terminal line, and terminal location (where applicable). It may also display plan and project files left by the user.

Finger—The traceroute or finger commands to run on the source machine (attacking machine) to gain more information about the attacker.

Fingerprint—a form of marking that embeds a unique serial number.

FIPS—Federal information processing standard.

Firewall—A device that forms a barrier between a secure and an open environment. Usually the open environment is considered hostile. The most notable open system s the Internet.

Firmware—Software or computer instructions that have been permanently encoded into the circuits of semiconductor chips.

FISMA—Federal Information Security Management Act.

FISSEA—The *Federal Information Systems Security Educator's Association*, an organization whose members come from federal agencies, industry, and academic institutions devoted to improving the IT security awareness and knowledge within the federal government and its related external workforce.

Fixed Wireless Access (FWA)—Replaces the last mile from the central office to the customer. This process usually consists of a pair of digital radio transmitters placed on rooftops, one at the central office and one at the users' site. These systems usually operate at the 38 Ghz portion of the spectrum. Also known as wireless fiber (because of the high speeds of throughput) and as fixed wireless local loop.

Flame—To express strong opinion or criticism of something, usually as a frank inflammatory statement in an electronic message.

Flat File—A collection of records containing no data aggregates, nested, or repeated data items, or groups of data items.

Flat-panel display—Thin lightweight monitor that takes up much less space than a CRT.

Flexibility—Responsiveness to change, specifically as it relates to user information needs and operational environment.

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

Floppy disk—A flexible removable disk used for magnetic storage of data, programs, or information.

FLR—Lifecycle support, flaw remediation.

FLS—Protection of the TSF, failure secure.

FLT—Resource utilization, fault tolerance.

FMBS—Frame-Mode Bearer Service.

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).

FMT—Security management functional class.

Force—A group of platforms and sites organized for a particular purpose.

Foreign Corrupt Practices Act—The act covers an organization's system of internal accounting control and requires public companies to make and keep books, records, and accounts that, in reasonable detail, accurately and fairly reflect the transactions and disposition of company assets and to devise and maintain a system of sufficient internal accounting controls. This act was amended in 1988.

Foreign Government Information—(1) Information provided to the United States by a foreign government or international organization of governments in the expectation, express or implied, that the information is to be kept in confidence. (2) Information, requiring confidentiality, produced by the United States pursuant to a written joint arrangement with a foreign government or international organization of governments. A written joint arrangement may be evidenced by an exchange of letters, a memorandum of understanding, or other written record of the joint arrangement.

Foreign key—A primary key of one file (relation) that appears in another file (relation).

Forensic Examination—After a security breach, the process of assessing, classifying and collecting digital evidence to assist in prosecution. Standard crime-scene standards are used.

Forensic image copy—An exact copy or snapshot of the contents of an electronic medium.

Forgery—A false, fake, or counterfeit datum, document, image, or act.

Formal analysis—The use of rigorous mathematical techniques to analyze a solution. The algorithms may be analyzed for numerical properties, efficiency, and correctness.

Formal design—The part of a software design written using a formal notation.

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. (2) The use of mathematical techniques in the specification, design, and analysis of computer hardware and software. .

Formal notation—The mathematical notation of a formal method. .

Formal proof—The discharge of a proof obligation by the construction of a complete mathematical proof. .

Formal Review—A type of review typically scheduled at the end of each activity or stage of development to review a component of a deliverable or, in some cases, a complete deliverable or the software product and its supporting documentation.

Formal specification—The part of the software specification written using a formal notation. .

Format—The physical arrangement of data characters, fields, records, and files.

Formerly Restricted Data—Information removed from the restricted data category upon determination jointly by the Department of Energy and Department of Defense that such information relates primarily to the military utilization of atomic weapons and that such information can be adequately safeguarded as classified defense information subject to the restrictions on transmission to other countries and regional defense organizations that apply to restricted data.

Formula Translation (Fortran)—A high-level programming language developed primarily to translate mathematical formulas into computer code.

Formulary—A technique for permitting the decision to grant or deny access to be determined dynamically at access time rather than at the time the access list is created.

Fortran—See Formula Translation.

Forum of Incident Response and Security Teams (FIRST)—A unit of the Internet Society that coordinates the activities of worldwide Computer Emergency Response Teams, regarding security-related incidents and information sharing on Internet security risks.

Fourier transform—An image processing tool which is used to decompose an image into its constituent parts or to view a signal in either the time or frequency domain.

Fourth-Generation Language (4GL)—A computer language that is easy to learn and use and often associated with rapid applications development.

FPA—Federal Privacy Act.

FPR—Privacy functional class.

FPT —Protection of the TSF functional class.

FRAD—Frame Relay Access Device.

Fragile watermark—A watermark that is designed to prove authenticity of an image or other media. A fragile watermark is destroyed, by design, when the cover is manipulated digitially. If the watermark is still intact then the cover has not been tampered with. Fragile watermark technology could be useful in authenticating evidence or ensuring the accuracy of medical records or other sensitive data. .

Fragment—A piece of a packet. When a router is forwarding an IP packet to a network with a Maximum Transmission Unit smaller than the packet size, it is forced to break up that packet into multiple fragments. These fragments will be reassembled by the IP layer at the destination host.

Fragmentation—The process in which an IP datagram is broken into smaller pieces to fit the requirements of a given physical network. The reverse process is termed "reassembly.".

Frame Relay—A switching interface that operates in packet mode. Generally regarded as the replacement for X.25.

Framework—Defines a set of application programming interface (API) classes for developing applications and for providing system services to those applications.

Free electrons—Electrons that are not attached to an atom or molecule. Also known as static electricity.

Free space and atmospheric attenuation—Defined by the loss the signal undergoes traveling through the atmosphere. Changes in air density and absorption by atmospheric particles are principle reasons for affecting the microwave signal in a free air space.

Frequency—The rate at which an electromagnetic waveform alternates, usually measured in Hertz.

Frequency diversity—A form of backup used to protect a radio signal. A second signal continually operates on a separate frequency and assumes the load when the regular channel fails.

Frequency Division Multiple Access (FDMA)—FDMA is the allocation of specific channels within a defined radio frequency bandwidth to carry a specific user's information. FDMA is a mature, reliable method of RF communication, but requires more spectrum than competing technologies to deliver its payload. .

Frequency Division Multiplexing (FDM)—An older technique in which the available transmission bandwidth of a circuit is divided by frequency into narrow bands, each used for a separate voice or data transmission channel, which many conversations can be carried on one circuit.

Frequency domain—A way of representing a signal where the horizontal deflection is the frequency variable and the vertical deflection is the signals amplitude at that frequency.

Frequency masking—A condition where two tones with relatively close frequencies are played at the same time and the louder tone masks the quieter tone. .

Frequency Modulation (FM)—A modulation technique in which the carrier frequency is shifted by an amount proportional to the value of the modulating signal. The amplitude of the carrier signal remains constant. The information signal causes the carrier signal to increase or decrease its frequency based on the waveform of the information signal.

Front office space—The primary interface to customers and sales channels.

Front Porch—The access point to a secure network environment; also known as a firewall.

Front-End Computer—A computer that offloads input and output activities from the central computer so it can operate primarily in a processing mode; sometimes called a front-end processor.

Front-End Processor (FEP)—(1) A communications computer associated with a host computer can perform line control, message handling, code conversion, error control, and application functions. (2) A teleprocessing concentrator and router, as opposed to a back-end processor or a database machine.

FRU—Resource utilization functional class.

FSIP—Fast serial interface processor.

FSK—Frequency shift keying.

FSP—Development, functional specification.

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. 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.

FTP—Trusted path/channels functional class.

FTP (File Transfer Protocol) server—Maintains a collection of files that can be downloaded.

Full Operational Capability (FOC)—The time at which a new system has been installed at all planned locations and has been fully integrated into the operational structure.

Full wave rectifier—Diodes designed to be placed in an alternating current circuit and to convert alternating current into direct current.

Full-Duplex (FDX)—An asynchronous communications protocol that allows the communications channel to transmit and receive signals simultaneously.

Fully Qualified Domain Name (FQDN)—A complete Internet address, including the complete host and domain name.

FUN—Tests, functional tests.

Function—In computer programming, a processing activity that performs a single identifiable task.

Functional Analysis—Translating requirements into operational and systems functions and identifying the major elements of the system and their configurations and initial functional design requirements.

Functional Domain—An identifiable DoD functional mission area. For purposes of the DoD policy memorandum, the functional domains are: command and control, space, logistics, transportation, health affairs, personnel, financial services, public works, research and development, and Intelligence, Surveillance, and Reconnaissance (ISR).

Functional Requirements—Architectural atoms; the elementary building blocks of architectural concepts; made up of activities/functions, attributes associated with activities/processes and processes/methods sequencing activities.

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.

Functional specification—The main product of systems analysis, which presents a detailed logical description of the new system. It contains sets of input, processing, storage, and output requirements specifying what the new system can do.

Functional testing—The segment of security testing in which the advertised security mechanisms of the system are tested, under operational conditions, for correct operation.

Functionality—Degree of acceptable performance of an act.

GAO— General Accounting Office.

Garbage Collection—A language mechanism that automatically deallocates memory for objects that are not accessible or referenced.

Gateway—A product that enables two dissimilar networks to communicate or interface with each other. In the IP community, an older term referring to a routing device. Today, the term “router” is used to describe nodes that perform this function, and “gateway” refers to a special-purpose device that performs an application layer conversion of information from one protocol stack to another. *Compare with* router.

GEN—Security audit generation.

General Support System—An interconnected information resource under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, facilities, and people and provides support for a variety of users and applications. Individual applications support different mission-related functions. Users may be from the same or different organizations.

General-Purpose Computer—A computer that can be programmed to perform a wide variety of processing tests.

Genetic algorithm—An artificial intelligence system that mimics the evolutionary, survival-of-the-fittest process to generate increasingly better solutions to a problem.

Geographic Information System (GIS)—A decision support system designed specifically to work with spatial information.

GIF—Graphics Interchange Format.

Gigabyte (G byte)—The equivalent of one billion bytes.

Gigahertz—The number of billions of CPU cycles per second.

GIGO—Garbage in, garbage out.

GII—Global information infrastructure.

GLBA—The Gramm-Leach-Bliley Act.

Global digital divide—The term used specifically to describe differences in IT access and capabilities between different countries or regions of the world.

Global economy—One in which customers, businesses, suppliers, distributors, and manufacturers operate without regard to physical and geographical boundaries.

Global Information Grid—The globally interconnected, end-to-end set of information capabilities, associated processes and personnel for collecting, processing, storing, disseminating and managing information on demand to warfighters, policy makers, and support personnel. The GiG includes all owned and leased communications and computing systems, services, software (including applications), data, security services and other associated services necessary to achieve Information Superiority.

Global Information Grid Architecture—The architecture, composed of interrelated operational, systems and technical views, which defines the characteristics of and relationships among current and planned Global Information Grid assets in support to National Security missions.

Global positioning system—A collection of 24 earth-orbiting satellites that continuously transmit radio signals to determine an object or target's current longitude, latitude, speed, and direction of movement.

Global reach—The ability to extend a company's reach to customers anywhere through an Internet connection and at a lower cost.

Glove—An input device that captures and records the shape, movement, and strength of the users' hands and fingers.

GNS—Get Nearest Server (Novell).

GOSIP—Government OSI Profile (U.S.).

Governing Security Requisites—Those security requirements that must be addressed in all systems. These requirements are set by policy, directive, or common practice; e.g., by Executive Order, Office of Management and Budget (OMB), Office of the Secretary of Defense, a Military Service or DoD Agency. Governing security requisites are typically high-level requirements. While implementations will vary from case to case, these requisites are fundamental and must be addressed.

Government OSI Profile (GOSIP)—A U.S. Government procurement specification for OSI protocols.

Government to business (G2B)—The E-commerce activities performed between a government and its business partners for purposes such as purchasing materials or soliciting and accepting bids for work.

Government to consumer (G2C)—The E-commerce activities performed between a government and its citizens or consumers, including paying taxes and providing information and services.

Government to government (G2G)—The E-commerce activities limited to a single nation's government focusing on vertical integration (local, city, state, and federal) and horizontal integration (within the various branches and agencies).

GPKI—Global public key infrastructure.

Graceful degradation—See *degraded-mode operation.*

Grand Design Program Strategies—Characterized by acquisition, development, and deployment of the total functional capability in a single increment.

Granularity—The level of detail contained in a unit of data. The more there is, the lower the level of granularity; the less detail, the higher the level of granularity.

Graphical User Interface (GUI)—An interface in which the user can manipulate icons, windows, pop-down menus, or other related constructs. A graphical user interface uses graphics such as a window, box, and menu to allow the user to communicate with the system. Allows users to move in and out of programs and manipulate their commands using a pointing device (usually a mouse). Synonymous with *user interface.*

Graphics output—Computer-generated output in the form of pictures, charts, and line drawings.

Graphics software—Helps the user create and edit photos and art.

Graphics terminal—An output device that displays pictures, charts, and line drawings, typically a high-resolution CRT.

GRE—Generic Routing Encapsulation.

Grid computing—Harnesses computers together by way of the Internet or a virtual network to share CPU power, databases, and storage.

Group document databases—A powerful storage facility for organizing and managing all documents relayed to specific teams.

Group Health Plan—Under HIPAA, an employee welfare benefit plan that provides for medical care and that either has 50 or more participants or is administered by another business entity. Also see Part II, 45 CFR 160.103.

Groupware—Software designed to function over a network to allow several people to work together on documents and files.

GSM—Originally stood for Groupe Speciale Moble, but is now known as Global System for Mobile Communications. It is the standard for cellular phone service in Europe, Japan, and Australia, and will soon be the standard for 30 to 50 percent of the cellular networks in the Untied States.

Guaranteed service—A service model that provides highly reliable performance with little or no variance in the measured performance criteria.

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

GUI (Graphical User Interface) screen design—The ability to model the information system screens for an entire system.

Guidelines—Documented suggestions for regular and consistent implementation of accepted practices. They usually have less enforcement powers.

GZL—Get Zone List (AppleTalk).

Hacker—A person who attempts to break into computers that he or she is not authorized to use.

Hacking—A computer crime in which a person breaks into an information system simply for the challenge of doing so.

Hacktivist—A politically motivated hacker who uses the Internet to send a political message of some kind.

HAG—High assurance guard.

Half-Duplex—Capability for data transmission in only one direction at a time between a sending station and a receiving station.

Half-duplex—A circuit designed for data transmission in both directions but not at the same time.

Halon—An abbreviation for halogenated hydrocarbon coined by the U.S. Army Corps of Engineers. Halon nomenclature follows the following rule: if a hydrocarbon compound contains the elements CaFbClcBrdIe, it is designated as Halon abcde (terminal zeros are dropped). Thus, Halon 1211 is chlorobromodifluoromethane, etc.

Handoffs (or switching)—A cellular call is switched from one cell tower to another as the user moves from one area to the next. The switch is usually unnoticed by the user.

Handover interface—A physical and logical interface across which the interception measures are requested from the NWO/AP/service provider, and the results of interception are delivered from a NWO/AP/service provider (SvP) to an LEMF.

Handprint Character Recognition (HCR)—One of several pattern recognition technologies used by digital imaging systems to interpret handprinted characters.

Handshake—Sequence of messages exchanged between two or more network devices to ensure transmission synchronization.

Handshaking Procedure—Dialogue between a user and a computer, two computers, or two programs to identify a user and authenticate his or her identity. This is done through a sequence of questions and answers that are based on information either previously stored in the computer or supplied to the computer by the initiator of the dialogue.

Handspring—A type of PDA that runs on the Palm Operating System (Palm OS).

Hard Disk—A fixed or removable disk mass storage system permitting rapid direct access to data, programs, or information.

Hard handoff—Sometimes a cell phone user being switched from one site to the next will need to be disconnected and reconnected to make the switch possible. Also called a “break and make” handoff, it is usually unnoticed by the user.

Hardware—The physical components of a computer network.

Hardware key logger—A hardware device that captures keystrokes on their way from the keyboard to the motherboard.

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.

Hash—Producing *hash values* for accessing data or for security. A hash value (or simply *hash*), also called a *message digest*, is a number generated from a string of text. The hash is substantially smaller than the text itself, and is generated by a formula in such a way that it is extremely unlikely that some other text will produce the same hash value. Hashing is also a common method of accessing data records. To create an index, called a *hash table,* for these records, you would apply a formula to each name to produce a unique numeric value.

Hash function/hashing—A hash function is a mathematical process based on an algorithm which creates a digital representation or compressed form of the message. It is often referred to as the message digest in the form of a hash value or hash result of a standard length which is usually much smaller than the message, but nevertheless substantially unique to it.

Hash Total—A total of the values on one or more fields, used for the purpose of auditability and control.

Hazard—A source of potential harm or a situation with potential to harm. 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.

HCFA—See the Health Care Financing Administration. Also see Part II, 45 CFR 160.103.

HCFA Common Procedural Coding System (HCPCS)—A medical code set that identifies healthcare procedures, equipment, and supplies for claim submission purposes. It has been selected for use in the HIPAA transactions. HCPCS Level I contains numeric CPT codes that are maintained by the AMA. HCPCS Level II contains alphanumeric codes used to identify various items and services that are not included in the CPT medical code set. These are maintained by HCFA, the BCBSA, and the HIAA. HCPCS Level III contains alphanumeric codes that are assigned by Medicaid state agencies to identify additional items and services not included in levels I or II. These are usually called “local” codes, and must have “W,” “X,” “Y,” or “Z” in the first position.

HCPCS Procedure Modifier Codes can be used with all three levels, with the WA-ZY range used for locally assigned procedure modifiers.

HCFA-1450—HCFA's name for the institutional uniform claim form, or UB-92.

HCFA-1500—HCFA's name for the professional uniform claim form. Also known as the UCF-1500.

HCPCS—See HCFA Common Procedural Coding System. Also see Part II, 45 CFR 162.103.

HDLC (High-Level Data-Link Control)—Bit-oriented synchronous datalink layer protocol developed by ISO. Derived from SDLC, HDLC specifies a data encapsulation method on synchronous serial links using frame characters and checksums.

HDSL—High-data-rate digital subscriber line. One of four DSL technologies. HDSL delivers 1.544 Mbps of bandwidth each way over two copper twisted pairs. Because HDSL provides T1 speed, telephone companies have been using HDSL to provision local access to T1 services whenever possible. The operating range of HDSL is limited to 12,000 feet (3658.5 meters), so signal repeaters are installed to extend the service. HDSL requires two twisted pairs, so it is deployed primarily for PBX network connections, digital loop carrier systems, interexchange POPs, Internet servers, and private data networks. *Compare with* ADSL, SDSL, and VDSL.

Header—The beginning of a message sent over the Internet; typically contains addressing information to route the message or packet to its destination.

Heading tag—HTML tag that puts certain information, such as the title, at the top of the page.

Headset—It combines input and output devices that (1) capture and record the movements of the user's head, and (2) contains a screen that covers the user's field of vision and displays various views of an environment based on the head's movements.

Health and Human Services (HHS)—The federal government department that has overall responsibility for implementing HIPAA.

Health Care—See Part II, 45 CFR 160.103.

Health Care Clearinghouse—Under HIPAA, this is an entity that processes or facilitates the processing of information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction, or that receives a standard transaction from another entity and processes or facilitates the processing of that information into nonstandard format or nonstandard data content for a receiving entity. Also see Part II, 45 CFR 160.103.

Health Care Code Maintenance Committee—An organization administered by the BCBSA that is responsible for maintaining certain coding schemes used in the X12 transactions and elsewhere. These include the Claim Adjustment Reason Codes, the Claim Status Category Codes, and the Claim Status Codes.

Health Care Component—See Part II, 45 CFR 164.504.

Health Care Financing Administration (HCFA)—The HHS agency responsible for Medicare and parts of Medicaid. HCFA has historically maintained the UB-92 institutional EMC format specifications, the professional EMC NSF specifications, and specifications for various certifications and authorizations used by the Medicare and Medicaid programs. HCFA also maintains the HCPCS medical code set and the Medicare Remittance Advice Remark Codes administrative code set.

Health Care Operations—See Part II, 45 CFR 164.501.

Health Care Provider—See Part II, 45 CFR 160.103.

Health Care Provider Taxonomy Committee—An organization administered by the NUCC that is responsible for maintaining the Provider Taxonomy coding scheme used in the X12 transactions. The detailed code maintenance is done in coordination with X12N/TG2/WG15.

Health Industry Business Communications Council (HIBCC)—A council of healthcare industry associations that has developed a number of technical standards used within the healthcare industry.

Health Informatics Standards Board (HISB)—An ANSI-accredited standards group that has developed an inventory of candidate standards for consideration as possible HIPAA standards.

Health Information—See Part II, 45 CFR 160.103.

Health information clearinghouses—Any public or private entities that process or facilitate processing nonstandard health information into standard data elements. For example, third party administrators; pharmacy benefits managers; billing services; information management and technology vendors; and others. (HIPAA).

Health Insurance Association of America (HIAA)— An industry association that represents the interests of commercial healthcare insurers. The HIAA participates in the maintenance of some code sets, including the HCPCS Level II codes.

Health Insurance Issuer—See Part II, 45 CFR 160.103.

Health Insurance Portability and Accountability Act of 1996 (HIPAA)—A federal law that allows persons to qualify immediately for comparable health insurance coverage when they change their employment relationships. Title II, Subtitle F, of HIPAA gives HHS the authority to mandate the use of standards for the electronic exchange of healthcare data; to specify what medical and administrative code sets should be used within those standards; to require the use of national identification systems for healthcare patients, providers, payers (or plans), and employers (or sponsors); and to specify the types of measures required to protect the security and privacy of personally identifiable healthcare information. Also known as the Kennedy-Kassebaum Bill, the Kassebaum-Kennedy Bill, K2, or Public Law 104-191.

Health Level Seven (HL7)—An ANSI-accredited group that defines standards for the cross-platform exchange of information within a healthcare organization. HL7 is responsible for specifying the Level Seven OSI standards for the health industry. The X12 275 transaction will probably incorporate the HL7 CRU message to transmit claim attachments as part of a future HIPAA claim attachments standard. The HL7 Attachment SIG is responsible for the HL7 portion of this standard.

Health Maintenance Organization (HMO)—See Part II, 45 CFR 160.103.

Health Oversight Agency—See Part II, 45 CFR 164.501.

Health Plan—See Part II, 45 CFR 160.103.

Health Plan ID—See National Payer ID.

Health plans—Individual or group plans (or programs) that provide health benefits directly, through insurance, or otherwise. For example, Medicaid; State Children's Health Insurance Program (SCHIP); state employee benefit programs; Temporary Assistance for Needy Families (TANF); and others. (HIPAA).

Healthcare Financial Management Association (HFMA)—An organization for the improvement of the financial management of healthcare-related organizations. The HFMA sponsors some HIPAA educational seminars.

Healthcare Information Management Systems Society (HIMSS)—A professional organization for healthcare information and management systems professionals.

Healthcare providers—Providers (or suppliers) of medical or other health services or any other person furnishing health care services or supplies, and who also conduct certain health-related administrative or financial transactions electronically. For example, local health departments; community and migrant health centers; rural health clinics; school-based health centers; homeless clinics and shelters; public hospitals; maternal and child health programs (Title V); family planning programs (Title X); HIV/AIDS programs; and others. (HIPAA).

HEDIC—The Healthcare EDI Coalition.

HEDIS—Health Employer Data and Information Set.

Help desk—Responds to knowledge workers' questions.

HERF—High-energy radio frequency.

Hertz—The basic measurement of bandwidth frequency in cycles per second. 1 Hertz equals 1 cycle per second.

Hertz (Hz)—One cycle per second.

Heuristics—The mode of analysis in which the next step is determined by the results of the current step of analysis. Used for decision support processing.

Hexadecimal—A number system with a base of 16.

HFMA—See the Healthcare Financial Management Association.

HHA—Home Health Agency.

HHIC—The Hawaii Health Information Corporation.

HHS—See Health and Human Services. Also see Part II, 45 CFR 160.103.

HIAA—See the Health Insurance Association of America.

HIBCC—See the Health Industry Business Communications Council.

Hidden partition—A method of hiding information on a hard drive where the partition is considered unformatted by the host operating system and no drive letter is assigned. .

HIDS—Host-based intrusion detection system.

Hierarchical Database—In a hierarchical database, data is organized like a family tree or organization chart with branches of parent records and child records.

High capacity floppy disk—Storage device that holds between 100MB and 250MB of information. Superdisks and Zip disks are examples.

High-Level Data-Link Control (HDLC)—A protocol used at the data-link layer that provides point-to-point communications over a physical transmission medium by creating and recognizing frame boundaries.

High-Level Language—The class of procedure-oriented language.

HIMSS—See the Healthcare Information Management Systems Society.

HIPAA Act of 1996—The Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA, Title II) require the Department of Health and Human Services to establish national standards for electronic healthcare transactions and national identifiers for providers, health insurers, and employers. It also addresses the security and privacy of health data. Adopting these standards will improve the efficiency and effectiveness of the nation's healthcare system by encouraging the widespread use of electronic data interchange in healthcare.

HIPAA Data Dictionary or HIPAA DD—A data dictionary that defines and cross-references the contents of all X12 transactions included in the HIPAA mandate. It is maintained by X12N/TG3.

HISB—See the Health Informatics Standards Board.

HL7—See Health Level Seven.

HLD—Development, high-level design.

HMO—See Health Maintenance Organization.

Holographic device—A device that creates, captures, and displays images in true three-dimensional form.

Home Page—The initial screen of information displayed to the user when initiating the client or browser software or when connecting to a remote computer. The home page resides at the top of the directory tree.

Home PNA (Home Phoneline Networking Alliance)—Allows one to network home computer using telephone wiring.

Homeland Security Act of 2002—The Act restructures and strengthens the executive branch of the federal government to better meet the threat to the United States posed by terrorism. In establishing a new department of Homeland Security, the Act for the first time creates a Federal department whose primary mission will be to help prevent, protect against, and respond to acts of terrorism on the U.S. soil.

Honey-pots—A specifically configured server, designed to attract intruders so their actions do not affect production systems; also known as a decoy server.

Hop—A term used in routing. A hop is one data link. A path from source to destination in a network is a series of hops.

Horizontal market software—Application software that is general enough to be suitable for use in a variety of industries.

Host—A remote computer that provides a variety of services, typically to multiple users concurrently.

Host Address—The IP address of the host computer.

Host Computer—A computer that, in addition to providing a local service, acts as a central processor for a communications network.

Hostname—The name of the user computer on the network.

Hot Site—A fully operational offsite data processing facility equipped with both hardware and system software to be used in the event of disaster.

Hot standby—Secondary equipment in place as a back up in case of primary equipment failure.

HPAG— The HIPAA Policy Advisory Group, a BCBSA subgroup.

HPSA— Health Professional Shortage Area.

HSRP—Hot Standby Routing Protocol.

HSSI—High-speed serial interface.

HTML—See *HyperText Markup Language.*

HTML document—A file made from the HTML language.

HTML tag—Specifies the formatting and presentation of information in an HTML document.

HTTP—See *HyperText Transport Protocol.*

Hub—A device connected to several other devices. In ARCnet, a hub is used to connect several computers together. In a message-handling service, a hub is used for transfer of messages across the network. An Ethernet hub is basically a “collapsed network-in-a-box” with a number of ports for the connected devices.

Humanware—Computer programs that interface or communicate with users by means of voice-integrated technology, interpret user-specified command, and execute or translate commands into machine-executable code.

HVAC—Heating ventilation air conditioning systems.

Hybrid Entity—A covered entity whose covered functions are not its primary functions. Also see Part II, 45 CFR 164.504.

Hypermedia—An extension to hypertext in which frames contain graphics, illustrations, images, audio, animation, text, and other forms of information or knowledge.

Hypertext—Text that is held in frames and authors develop or define the linkage between frames.

Hypertext Markup Language—A language created by programmers at the CERN in Switzerland to create Web pages.

HyperText Transfer Protocol (HTTP)—A communication protocol used to connect to serves on the world-wide-web. Its primary function is to establish a connection with a web server and transmit HTML pages to the client browser. The protocol used to transport hypertext files across the Internet.

I&A—Identification and authentication.

IA—(1) Information assurance. (2) Intra-area (OSPF).

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.

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.

IAB—Internet Architecture Board. Board of internetwork researchers who discuss issues pertinent to Internet architecture. Responsible for appointing a variety of Internet-related groups such as the IANA, IESG, and IRSG. The IAB is appointed by the trustees of the ISOC.

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.

IAIABC— See the International Association of Industrial Accident Boards and Commissions.

IAP—Information Awareness Program.

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.

IBGP—Interior Border Gateway Protocol.

ICD & ICD-n-CM & ICD-n-PCS—International Classification of Diseases, with "n" = "9" for Revision 9 or "10" for Revision 10, with "CM" = "Clinical Modification," and with "PCS" = "Procedure Coding System.".

ICF—Intermediate Care Facility.

ICMP—Internet Control Message Protocol. Network layer Internet protocol that reports errors and provides other information relevant to IP packet processing. Documented in RFC 792.

ICMP—Internet Control Message Protocol.

Icon—A pictorial symbol used to represent data, information, or a program on a GUI screen.

ICQ—Pronounced "I Seek You." This is a chat service available via the Internet that enables users to communicate online. This service (you load the application on your computer) allows chat via text, voice, bulletin boards, file transfers, and e-mail.

ICSA—Internet Computer Security Association.

ICZ—Intensive Control Zone.

IDA (infrared date association) port—A port for wireless devices that works in essentially the same way as the remote control on TV.

Identification—(1) The process, generally employing unique machine-readable names, that enables recognition of users or resources as identical to those previously described to the computer system. (2) The assignment of a name by which an entity can be referenced. The entity may be high level (such as a user) or low level (such as a process or communication channel.

Identification Media—A building or visitor pass.

Identifier—A set of one or more attributes that uniquely distinguishes each instance of an object.

Identity—Information that is unique within a security domain and which is recognized as denoting a particular entity within that domain.

Identity-based security policy—A security policy based on the identities or attributes of users, a group of users, or entities acting on behalf of the users and the resources or targets being accessed.

IDN—Integrated Delivery Network.

IDS—Intrusion detection system.

IEC 61025 —International Electrotechnical Commission Publication 61025 Fault tree analysis (FTA).

IEEE—Institute of Electrical and Electronics Engineers.

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

IETF—Internet Engineering Task Force.

IFC—User data protection information flow control policy.

IFF—User data protection information flow control functions.

IG—See *Implementation Guide.*

IGP—Interior Gateway Protocol.

IGRP—Interior Gateway Routing Protocol.

IGS—Delivery and operation, installation, generation, and start-up.

IHC—Internet Healthcare Coalition.

IIHI—See Individually Identifiable Health Information.

IKE—Internet Key Exchange protocol.

IMP—Development, implementation representation.

Impact—The amount of loss or damage that can be expected, or may be expected from a successful attack of an asset.

Impact printer—A hard-copy device on which a print mechanism strikes against a ribbon to create imprints on paper. Some impact printers operate one character at a time; others strike an entire line at a time.

Impersonation—An attempt to gain access to a system by posing as an authorized user.

Implant chip—A technology-enabled microchip implanted into the human body.

Implementation—The specific activities within the systems development life cycle through which the software portion of the system is developed, coded, debugged, tested, and integrated with existing or new software.

Implementation Guide (IG)—A document that explains the proper use of a standard for a specific business purpose. The X12N HIPAA IGs are the primary reference documents used by those implementing the associated transactions, and are incorporated into the HIPAA regulations by reference.

Implementation phase—Distributes the system to the knowledge workers who begin using the system in their everyday jobs.

Implementation Specification—Under HIPAA, this is the specific instruction for implementing a standard. Also see Part II, 45 CFR 160.103. See also *Implementation Guide.*

Importance—A subjective assessment of the significance of a system's capability and the consequences of the loss of that capability.

In band—Made up of tones that pass within the voice frequency band and are carried along the same circuit as the talk path established by the signals. Also known as in-band signaling.

Inadvertent Disclosure—Accidental exposure of information to a person not authorized access.

Inadvertent Loss—The unplanned loss or compromise of data or system.

Incident—An unusual occurrence or breach in the security of a computer system. An event that has actual or potentially adverse effects on an information system. A computer security incident can result from a computer virus, other malicious code, intruder, terrorist, unauthorized insider act, malfunction, etc.

Incomplete Parameter Checking—A system fault that exists when all parameters have not been fully checked for correctness and consistency by the operating system, thus leaving the system vulnerable to penetration.

Incremental Program Strategies—Characterized by acquisition, development, and deployment of functionality through a number of clearly defined system "increments" that stand on their own.

IND—Tests, independent testing.

Independent Basic Service Set Network (IBSS Network)—Independent Basic Service Set Network is an IEEE 802.11-based wireless network that has no backbone infrastructure and consists of at least two wireless stations. This type of network is often referred to as an ad hoc network because it can be constructed quickly without much planning.

Indexed sequential filing—A file organization method in which records are maintained in logical sequence and indices (or tables) are used to reference their storage addresses. The method allows direct and serial access to records.

Indirect material—Material that is necessary for running a modern corporation but does not relate to the company's primary business activities. Commonly called MRO materials.

Induction—A process of logically arriving at a conclusion about a member of a class from examining a few other members of the same class. This method of reasoning may not always produce true statements. As an example, suppose it is known that George's car has four tires and that Fred's car has four tires. Inductive reasoning would allow the conclusion that all cars have four tires. Induction is closely related to learning.

Inference Engine—A system of computer programs in an expert systems application that uses expert experience as a basis for conclusions.

Infobots—Software agents that perform specified tasks for a user or application.

Information—Intelligence or knowledge capable of being represented in forms suitable for communication, storage, or processing. Information may be represented, for example, by signs, symbols, pictures, or sounds.

Information age—A time when knowledge is power.

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 environments. (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 Assurance Support Environment (IASE)—The IASE is an on-line Web-based help environment for DoD INFOSEC and IA professionals.

Information Assurance Vulnerability Alert (IAVA)—The comprehensive distribution process for notifying CINC's, Services and agencies (C/S/A) about vulnerability alerts and countermeasures information. The IAVA process requires C/S/A receipt acknowledgment and provides specific time parameters for implementing appropriate countermeasures depending on the criticality of the vulnerability.

Information Attributes—The qualities, characteristics, and distinctive features of information.

Information Category—The term used to bind information and tie it to an information security policy.

Information decomposition—Breaking down the information for ease of use and understandability.

Information environment—The aggregate of individuals, organizations, and systems that collect, process, or disseminate information, including the information itself.

Information float—The amount of time it takes to get information from its source into the hands of the decision makers.

Information granularity—The extent of detail within the information.

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.

Information in identifiable form—Information in an IT system or online collection that (i) directly identifies an individual (e.g., name, address, Social Security number, or other identifying number or code, telephone number, e-mail address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors. .

Information Interoperability—The exchange and use of information in any electronic form.

Information Model—A conceptual model of the information needed to support a business function or process.

Information Operations (IO)—Actions taken to affect adversary information and information systems while defending one's own information and information systems.

Information Operations Condition (INFOCON)—The INFOCON is a comprehensive defense posture and response based on the status of information systems, military operations, and intelligence assessments of adversary capabilities and intent. The INFOCON system presents a structured, coordinated approach to defend against a computer network attack. INFOCON measures focus on computer network-based protective measures. Each level reflects a defensive posture based on the risk of impact to military operations through the intentional disruption of friendly information systems. INFOCON levels are: NORMAL (normal activity); ALPHA (increased risk of attack);

BRAVO (specific risk of attack); CHARLIE (limited attack); and DELTA (general attack). Countermeasures at each level include preventive actions, actions taken during an attack, and damage control/mitigating actions.

Information owner—An official having statutory or operational authority for specified information and having responsibility for establishing controls for its generation, collection, processing, dissemination, and disposal. .

Information partnership—Two or more companies that cooperate by integrating their IT systems, thereby providing customers with the best of what each has to offer.

Information requirements—Those items of information regarding the enemy and his environment which need to be collected and processed in order to meet the intelligence requirements of a commander.

Information resource management—A concept or practice in which information is recognized as a key asset to be appropriately managed as a vital resource.

Information Security—Safeguarding information against unauthorized disclosure; or, the result of any system of administrative policies and procedures for identifying, controlling, and protecting from unauthorized disclosure, information the protection of which is authorized by Executive Order or statute.

Information Security Governance—The management structure, organization, responsibility and reporting processes surrounding a successful information security program.

Information Security Program—The overall process of preserving confidentiality, integrity and availability of information.

Information Security Service—A method to provide some specific aspect of security. For example, integrity of transmitted data is a security objective, and a method that would achieve that is considered an information security service.

Information services—The offering of a capability for generating, storing, transforming, retrieving, utilizing, or making available information via telecommunications, and includes electronic publishing but does not include the use of such capability for the management, control, or operation of a telecommunications system or the management of a telecommunications service.

Information sharing—The requirements for information sharing by an IT system with one or more other IT systems or applications, for information sharing to support multiple internal or external organizations, missions, or public programs.

Information superiority—The capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. Forces attain information superiority through the acquisition of systems and families-of-systems that are secure, reliable, interoperable, and able to communicate across a universal Information Technology (IT) infrastructure, to include National Security Systems (NSS). This IT infrastructure includes the data, information, processes, organizational interactions, skills, and analytical expertise, as well as systems, networks, and information exchange capabilities.

Information system—A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. .

Information system owner (or program manager)—See system owner.

Information system security—A system characteristic and a set of mechanisms that span the system both logically and physically. .

Information system security officer—Individual responsible to the OA ISSO, designated approving authority, or information system owner for ensuring that the appropriate operational security posture is maintained for an information system or a closely related group of systems. .

Information Systems Security (INFOSEC)—The 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 or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats.

Information systems security program—Synonymous with *IT security program.*

Information Technology (IT)—The hardware and software operated by a federal agency or by a contractor of a federal agency or other organization that processes information on behalf of the federal government to accomplish a federal function, regardless of the technology involved, whether computers, telecommunications, or others. It includes automatic data processing equipment as that term is defined in Section 111(a)(2) of the Federal Property and Administrative Services Act of 1949. For the purposes of this Circular, automatic data processing and telecommunications activities related to certain critical national security missions, as defined in 44 U.S.C. 3502(2) and 10 U.S.C. 2315, are excluded.

Information technology disruptions due to natural or man-made disasters—Failure to exercise due care and diligence in the implementation and operation of the information technology system.

Information view—Includes all of the information stored within a system.

Information Warfare (IW)—Actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems and computer-based networks while defending one's own information, information-based processes, information systems and computer-based networks.

Information-literate knowledge workers—Can define what information they need, know how to obtain that information, understand the information once they receive it, and act appropriately to help the organization achieve the greatest advantage.

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.

Infrared—A wireless communications medium that uses light waves to transmit signals or information.

Infrastructure—The framework of interdependent networks and systems comprising identifiable industries, institutions, and distribution capabilities that provide a continual flow of goods and services essential to the defense and economic security of the United States, the smooth functioning of government at all levels, or society as a whole.

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. 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. .

Infrastructure-Centric—A security management approach that considers information systems and their computing environment as a single entity.

Inheritance—The language mechanism that allows the definition of a class to include the attributes and methods for another more general class. Inheritance is an implementation construct for the specialization relation. The general class is the superclass and the specific class is the subclass in the inheritance relation. Inheritance is a relation between classes that enables the reuse of code and the definition of generalized interface to one or more subclasses.

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. .

Initial Operational Capability (IOC)— The first time a new system is introduced into operation.

Initialization vector—A non-secret binary vector used as the initializing input algorithm for the encryption of a plaintext block sequence to increase security by introducing additional cryptographic variance and to synchronize cryptographic equipment.

Initiator—An entity (for example, human user or computer based entity) that attempts to access other entities.

Initiator access control decision information—ADI associated with the initiator.

Initiator access control information—Access control information relating to the initiator.

Injection—Using this method, a secret message is put in a host file in such a way that when the file is actually read by a given program, the program ignores the data.

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.

Inkjet printer—Makes images by forcing ink droplets through nozzles.

Inmate—See Part II, 45 CFR 164.501.

Input controls—Techniques and methods for verifying, validating, and editing data to ensure that only correct data enters a system.

Input device—A tool used to capture information and commands by the user.

Inquiry processing—The process of selecting a record from a file and immediately displaying its contents.

Insourcing—It means that IT specialists within the organization will develop the system.

Inspection—A manual analysis technique that examines the program requirements, design, or code in a formal and disciplined manner to discover errors.

Instance—A set of values representing a specific entity belonging to a particular entity type. A single value is also the instance of a data item.

Instance—An occurrence of an entity class that can be uniquely described.

Instrumental input—The capture of data and its placement directly into a computer by machines.

Insulator—A material that does not conduct electricity but is suitable for surrounding conductors to prevent the loss of current.

INT—(1) Protection Profile evaluation, PP introduction. (2) Security Target evaluation, ST introduction. (3) development, TSF internals.

Integrated circuit—A miniature microchip incorporating circuitry and semi-conductor components. The circuit elements and components are created as a part of the same manufacturing process.

Integrated Data Dictionary (IDD)—A database technology that facilitates functional communication among system components.

Integrated Services Digital Network (ISDN)—An emerging technology that is beginning to be offered by the telephone carriers of the world. ISDN combines voice and digital network services in a single medium, making it possible to offer customers digital data services as well as voice connections through a single wire. The standards that define ISDN are specified by ITU-TSS.

Integration—Allows separate systems to communicate directly with each other by automatically exporting data files from one system and importing them into another.

Integration testing—The orderly progression of testing in which software, hardware, or both are combined and tested until all intermodule communication links have been integrated.

Integrator—The organization that integrates the IS components.

Integrity—1. The accuracy, completeness and validity of information in accordance with business values and expectations. The property that data or information has not been modified or altered in an unauthorized manner. 2. A security service that allows verification that an unauthorized modification (including changes, insertions, deletions and duplications) has not occurred either maliciously or accidentally. *See also* data integrity.

Integrity checking—The testing of programs to verify the soundness of a software product at each phase of development.

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. (2) A range of values of a property of an item necessary to maintain risk exposure at or below its acceptability threshold. .

Intellectual property—Intangible creative work that is embodied in physical form.

Intellectual property identification—A method of asset protection which identifies or defines a copyright, patent, trade secret, etc. or validates ownership and ensures that intellectual property rights are protected.

Intellectual Property Management and Protection (IPMP) —A refinement of digital rights management (DRM) that refers specifically to MPEG's.

Intelligence—The first step in the decision making process where a problem, need, or opportunity is found or recognized. Also called the diagnostic phase of decision making.

Intelligence Method—The method which is used to provide support to an intelligence source or operation, and which, if disclosed, is vulnerable to counteraction that could nullify or significantly reduce its effectiveness in supporting the foreign intelligence or foreign counterintelligence activities of the United States, or which would, if disclosed, reasonably lead to the disclosure of an intelligence source or operation.

Intelligence Source—A person, organization, or technical means which provides foreign intelligence or foreign counterintelligence and which, if its identity or capability is disclosed, is vulnerable to counteraction that could nullify or significantly reduce its effectiveness in providing foreign intelligence or foreign counterintelligence to the United States. An intelligence source also means a person or organization which provides foreign intelligence or foreign counterintelligence to the United States only on the condition that its identity remains undisclosed.

Intelligent agent—Software that assists the user in performing repetitive computer-related tasks.

Intelligent cabling—Research is ongoing in this area. The goal is to eliminate the large physical routers, hubs, switches, firewalls, etc. and move these functions (i.e., embed the intelligence) into the cabling itself. Currently this is an electrochemical/neuronic research process.

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. .

Interactive—A mode of processing that combines some aspects of online processing and some aspects of batch processing. In interactive processing, the user can directly interact with data over which he or she has exclusive control. In addition, the user can cause sequential activity to initiate background activity to be run against the data.

Interactive chat—Lets the user engage in real-time exchange of information with one or more individuals over the Internet.

Interactive video —A system in which video segments are integrated via a menu-based processing application.

Interagency Coordination—Within the context of Department of Defense involvement, the coordination that occurs between elements of the Department of Defense and engaged U.S. government agencies, nongovernment organizations, private voluntary organizations, and regional and international organizations for the purpose of accomplishing an objective.

Interblock Gap (IBG)—A blank space appearing between records or groups of records on magnetic storage media.

Interception—Action (based on the law) performed by an NWO/AP/SvP, of making available certain information and providing that information to an LEMF. Usually, this term is not used to describe the action of observing communications directly by an LEA.

Interception interface—Physical and logical locations within the NWO/AP/SvP telecommunications facilities where access to the CC and IRI is provided. The interception interface is not necessarily a single fixed point.

Interception measure—A technical measure that facilitates the interception of telecommunications traffic pursuant to the relevant national laws and regulations.

Interception subject—A person or persons, specified in a lawful authorization, whose telecommunications are to be intercepted.

Intercept-related information—Collection of information or data associated with telecommunications services involving the target identity, specifically communication-associated information or data (including unsuccessful communication attempts), service-associated information or data (e.g., service-profile management by subscriber), and location information.

Interconnection security agreement—An agreement established between the organizations that own and operate connected information technology systems to document the technical requirements of the interconnection. The ISA also supports a memorandum of understanding or agreement (MOU/A) between the organizations. .

Interdiction—Impeding or denying someone the use of system resources.

Interface—A shared boundary between devices, equipment, or software components defined by common interconnection characteristics.

Interface analysis—The checking and verification process that ensures intermodule communications links are performed correctly.

Interference—Electromagnetic energy that is picked up with the signal you are receiving. This extra energy distorts the signal and interferes with its transmission.

Interim accreditation—Temporary authorization granted by a designated approving authority for an information technology system to process, store, and transmit information based on preliminary results of security certification of the system. .

Interim Approval to Operate (IATO)—Temporary approval granted by a DAA for an IS to process information based on preliminary results of a security evaluation of the system.

Interleaving—The alternating execution of programs residing in the memory of a multiprogramming environment.

Intermediary—A specialist company that provides services better than its client companies.

Internal accounting control—The process of safeguarding the accounting functions and processes of a business. This process includes validating that the accounting system complies with the appropriate, generally accepted accounting principles and that audit trails exist for verification of all processes.

Internal control—The method of safeguarding business assets, including verifying the accuracy and reliability of accounting data, promoting operational efficiency, and encouraging adherence to prescribed organizational policies and procedures.

Internal information—Information that describes specific operational aspects of the organization.

Internal network interface—Network's internal interface between the internal intercepting function and a mediation function.

International Association of Industrial Accident Boards and Commissions (IAIABC)— One of their standards is under consideration for use for the First Report of Injury standard under HIPAA.

International Classification of Diseases (ICD)— A medical code set maintained by the World Health Organization (WHO). The primary purpose of this code set was to classify causes of death. A U.S. extension, maintained by the NCHS within the CDC, identifies morbidity factors, or diagnoses. The ICD-9-CM codes have been selected for use in the HIPAA transactions.

International government-to-government (IG2G)—The E-commerce activities performed between two or more governments, including foreign aid.

International Organization—An organization of governments.

International Organization for Standardization (ISO)— An organization that coordinates the development and adoption of numerous international standards. "ISO" is not an acronym, but the Greek word for "equal.".

International Standards Organization— See International Organization for Standardization (ISO).

International virtual private network (IVPN)—Virtual private networks that depend on services offered by phone companies of various nationalities.

Internet—A global computer network that links minor computer networks, allowing them to share information via standardized communication protocols. The Internet consists of large national backbone networks (such as MILNET, NSFNET, and CREN) and a myriad of regional and local campus networks all over the world. The Internet uses the Internet Protocol suite. To be on the Internet, you must have IP connectivity (i.e., be able to Telnet to--or ping--other systems). Networks with only email connectivity are not actually classified as being on the Internet. Although it is commonly stated that the Internet is not controlled or owned by a single entity, this is really misleading, giving many users the perception that no one is really in control (no one "owns") the Internet. In practical reality, the only way the Internet can function is to have the major telecom switches, routers, satellite, and fiber optic links in place at strategic locations. These devices at strategic locations are owned by a few major corporations. At any time, these corporation could choose to shut down these devices (which would shut down the Internet), alter these devices so only specific countries or regions could be on the Internet, or modify these devices to allow/disallow/monitor any communications occurring on the Internet.

Internet address—A 32-bit address assigned to hosts using TCP/IP.

Internet Architecture Board (IAB)—Formally called the Internet Activities Board. The technical body that oversees the development of the Internet suite of protocols (commonly referred to as TCP/IP). It has two task forces (the IRTF and the IETF), each charged with investigating a particular area.

Internet Assigned Numbers Authority (IANA)—A largely government-funded overseer of IP allocations chartered by the FNC and the ISOC.

Internet backbone—The major set of connections for computers on the Internet.

Internet Control Message Protocol (ICMP)—The protocol used to handle errors and control messages at the IP layer. ICMP is actually part of the IP.

Internet Engineering Task Force (IETF)—The Internet standards setting organization with affiliates internationally from network industry representatives. This includes all network industry developers and researchers concerned with evolution and planned growth on the Internet.

Internet Layer—The stack in the TCP/IP protocols that addresses a packet and sends the packets to the network access layer.

Internet Message Access Protocol (IMAP)—A method of accessing electronic mail or bulletin board messages that are kept on a (possibly shared) mail server. IMAP permits a "client" email program to access remote message stores as if they were local. For example, email stored on an IMAP server can be manipulated from a desktop computer at home, a workstation at the office, and a notebook computer while traveling, without the need to transfer messages of files back and forth between these computers. IMAP can be regarded as the next-generation POP.

Internet Protocol (IP, lPv4)—The Internet Protocol (version 4), defined in RFC 791, is the network layer for the TCP/IP suite. It is a connectionless, best-effort, packet-switching protocol.

Internet Protocol (Ping, IPv6)—IPv6 is a new version of the Internet Protocol that is designed to be evolutionary.

Internet server computer—Computer that provides information and services on the Internet.

Internet Service Provider (ISP)—An organization that provides direct access to the Internet, such as the provider that links your college or university to the Net.

Internet telephony—A combination of hardware and software that uses the Internet as the medium for transmission of telephone calls in place of traditional telephone networks.

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

Interoperability—The ability to exchange requests between entities. Objects interoperate if the methods that apply to one object can request services of another object.

Interorganizational System (IOS)—Automates the flow of information between organizations to support the planning, design, development, production, and delivery of products and services.

Intersection relation—A relation the user creates to eliminate a many-to-many relationship. Also called a composite relation.

Intracell handovers—A cellular call is passed from one frequency to the next or carrier to the next within a single cell site.

Intranet—An internal organizational Internet that is guarded against outside access by a special security feature called a firewall.

Intrusion detection—The process of monitoring the events occurring in a computer system or network, detecting signs of security problems.

Intrusion-detection software—Looks for unauthorized users on the Internet.

Investigation—The phase of the systems development life cycle in which the problem or need is identified and a decision is made on whether to proceed with a full-scale study.

Invisible GIFs (Tracker GIF, Clear GIF)—Electronic images, usually not visible to site visitors, that allow a Web site to count those who have visited that page or to access certain cookies. .

Invisible ink—A method of steganography that uses a special ink that is colorless and invisible until treated by a chemical, heat, or special light. It is sometimes referred to as *sympathetic ink*.

Invisible watermark—An overlaid image which is invisible to the naked eye, but which can be detected algorithmically. There are two different types of invisible watermarks: fragile and robust.

IO—Information operations.

IOM—Institute of Medicine. Prestigious group of physicians that study issues and advise Congress. The IOM developed a report on computer-based patient records that led to the creation of CPRI. .

IOS—Internetwork Operating System.

IP—Internet Protocol.

IP Address—A unique number assigned to each computer on the Internet, consisting of four numbers, each less than 256, and each separated by a period, such as 129.16.255.0.

IP Datagram—The fundamental unit of information passed across the Internet. Contains source and destination addresses, along with data and a number of fields that define such things as the length of the datagram, the header checksum, and flags to say whether the datagram can be (or has been) fragmented.

IP security protocol (IPSec)—A protocol in development by the IETF to support secure data exchange. Once completed, IPSec is expected to be widely deployed to implement Virtual Private Networks (VPN). IPSec supports two encryption modes: Transport and Tunnel. Transport mode encrypts the data portion (payload) of each packet but leaves the header untouched. Tunnel mode is more secure since in encrypts both the header and the payload. On the receiving side, an IPSec-compliant device decrypts each packet.

IP Spoofing—IP (Address) Spoofing is a technique used to gain unauthorized access to computers or network devices, whereby the intruder sends messages with an IP source address to pretend that the message is coming from a trusted source.

IPA— Independent Providers Association.

IPC—Inter-process communication.

IPL—Initial program load.

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.

IPX—Internet packet exchange.

IRB—Integrated routing and bridging.

IRB— Institutional Review Board.

IRC—Internet Relay Chat. This is a service (you must load the application on your computer) that allows interactive conversation on the Internet. IRC also allows you to exchange files and have "private" conversations. Some major supporters of this service are IRCnet and DALnet.

IS—Intermediate system.

IS Security Goal—See *Security Goal.*

ISACA—Information Systems Audit and Control Association.

ISAKMP—Internet Security Association Key Management Protocol.

(ISC)^2—International Information Systems Security Certification Consortium.

ISDN (Integrated Services Digital Network)—There are two forms of ISDN: PRI and BRI. BRI interface supports a total signaling rate of 144 kbps, which is divided up into two B or bearer channels, which run at 64 kbps, and a D or data channel, which runs at 16 kbps. The bearer channels carry the actual voice, video, or data information, and the D channel is used for signaling. PRI or primary rate interface provides the same throughput as a T-1 1.544 Mbps, has 23 B or bearer channels, which run at 64 kbps, and a D or data channel, which runs at 16 kbps.

ISDN BRI—Integrated Services Digital Network — Basic Rate Interface.

ISDN PRI—Integrated Services Digital Network — Primary Rate Interface.

ISIS—Intermediate System Intermediate System (OSI standard routing protocol).

ISM (Industrial, Scientific, and Manufacturing) frequencies—A term describing several frequencies in the radio spectrum set aside for specific purposes.

ISO— See the International Organization for Standardization.

ISO 17799—ISO 17799 gives general recommendations for information security management. It is intended to provide a common international basis for developing organizational security standards and effective security management practice and to provide confidence in inter-organizational dealings.

ISO 9000—A certification program that demonstrates an organization adheres to steps that ensure quality of goods and services. A quality series that comprises a set of five documents and was developed in 1987 by the International Standards Organization (ISO).

Isolation—The separation of users and processes in a computer system from one another, as well as from the protection controls of the operating system.

ISP—See Internet Service Provider. .

IS-Related Risk—The probability that a particular threat agent will exploit, or trigger, a particular information system vulnerability and the resulting mission/business impact if this should occur. IS related-risks arise from legal liability or mission/business loss due to (1) Unauthorized (malicious, nonmalicious, or accidental) disclosure, modification, or destruction of information; (2) Nonmalicious errors and omissions; (3) IS disruptions due to natural or man-made disasters; (4) Failure to exercise due care and diligence in the implementation and operation of the IS.

ISSA—Information Systems Security Association.

ISSO—Information system security officer.

IT infrastructure—The hardware, software, and telecommunications equipment that when combined provides the underlying foundation to support the organization's goal.

IT security—Technological discipline concerned with ensuring that IT systems perform as expected and do nothing more; that information is provided adequate protection for confidentiality; that system, data and software integrity is maintained; and that information and system resources are protected against unplanned disruptions of processing that could seriously impact mission accomplishment. Synonymous with *Automated information system security, Computer security* and *information systems security.*

IT security architecture—A description of security principles and an overall approach for complying with the principles that drive the system design; i.e., guidelines on the placement and implementation of specific security services within various distributed computing environments.

IT security basics—A core set of generic IT security terms and concepts for all federal employees as a baseline for further, role-based learning.

IT security body of knowledge topics and concepts—A set of 12 high-level topics and concepts intended to incorporate the overall body of knowledge required for training in IT security.

IT security goals—See *security goals.*

IT security literacy—The first solid step of the IT security training level where the knowledge obtained through training can be directly related to the individual's role in his or her specific organization.

IT security program—A program established, implemented, and maintained to assure that adequate IT security is provided for all organizational information collected, processed, transmitted, stored, or disseminated in its information technology systems. Synonymous with *Automated information system security program, Computer security program,* and *information systems security program.*

IT system—a collection of computing or communications components and other resources that support one or more functional objectives of an organization. IT system resources include any IT component plus associated manual procedures and physical facilities that are used in the acquisition, storage, manipulation, display, or movement of data or to direct or monitor operating procedures. An IT system may consist of one or more computers and their related resources of any size. The resources that comprise a system do not have to be physically connected.

ITA—Protection of the TSF, availability of exported TSF data.

ITC—(1) User data protection, import from outside TSF control; (2) protection of the TSF, confidentiality of exported TSF data; (3) trusted path/channels, inter-TSF trusted channel.

Iterative Development Life Cycle—A strategy for developing systems that allows for the controlled reworking of parts of a system to remove mistakes or to make improvements based on feedback.

ITL—Information Technology Laboratory.

IT-Related Risk—The net mission/business impact considering the probability that a particular threat source will exploit, or trigger, a particular information system vulnerability, and the resulting impact if this should occur. IT-related risks arise from legal liability or mission/business loss due to, but not limited to (1) Unauthorized (malicious, nonmalicious, or accidental) disclosure, modification, or destruction of information; (2) Nonmalicious errors and omissions; (3) IT disruptions due to normal or man-made disasters; (4) Failure to exercise due care and diligence in the implementation and operation of the IT.

ITS—Intelligent transportation systems.

ITSEC—Information Technology Security Evaluation Criteria.

ITT—(1) User data protection, internal TOE transfer. (2) protection of the TSF, internal TOE TSF data transfer.

ITU—International Telecommunications Union.

ITU-T—ITU Telecommunication Standardization Sector.

IW—Information warfare.

Jargon code—A code that uses words (esp. nouns) instead of figure or letter-groups as the equivalent of plain language units.

Java—Object-oriented programming language developed at Sun Microsystems to solve a number of problems in modern programming practice. The Java language is used extensively on the World Wide Web, particularly for applets.

JCAHO—See the Joint Commission on Accreditation of Healthcare Organizations.

J-Codes—A subset of the HCPCS Level II code set with a high-order value of "J" that has been used to identify certain drugs and other items. The final HIPAA transactions and code sets rule states that these J-codes will be dropped from the HCPCS, and that NDC codes will be used to identify the associated pharmaceuticals and supplies.

JHITA—See the Joint Healthcare Information Technology Alliance.

Jitter attack—A method of testing or defeating the robustness of a watermark. This attack applies "jitter" to a cover by splitting the file into a large number of samples, the deletes or duplicates one of the samples and puts the pieces back together. At this point the location of the embedded bytes cannot be found. This technique is nearly imperceptable when used on audio and video files.

Job—A complete set of programs to be executed in sequence on a computer.

Job accounting system—A set of systems software that can track the services and resources used by computer system account holders.

Job function—The roles and responsibilities specific to an individual, not a job title.

Job queue—A set of programs held in temporary storage and awaiting execution.

Join—An operation that takes two relations as operand and produces a new relation by concealing the tuples and matching the corresponding columns when a stated condition holds between the two.

Joint Application Development (JAD)—Occurs when knowledge workers and IT specialists meet, sometimes for several days, to define or review the business requirements for the system.

Joint Commission on Accreditation of Healthcare Organizations (JCAHO)—An organization that accredits healthcare organizations. In the future, the JCAHO may play a role in certifying these organizations' compliance with the HIPAA A/S requirements.

Joint Healthcare Information Technology Alliance (JHITA)—A healthcare industry association that represents AHIMA, AMIA, CHIM, CHIME, and HIMSS on legislative and regulatory issues affecting the use of health information technology.

JPEG—Joint Photographic Experts Group.

Judgment—The ability to make a decision or form an opinion by discerning and evaluating.

Jukebox—Hardware that houses, reads, and writes to many optical disks using a variety of mechanical methods for operation.

Just in Time (JIT)—An approach that produces or delivers a product or service just at the time the customer wants it.

KDC—Key distribution center.

Kerberos—Developing standard for authenticating network users. Kerberos offers two key benefits: it functions in a multi-vendor network, and it does not transmit passwords over the network.

Kerckhoff's principle—A cryptography principle that states if the method used to encipher data is known by an opponent then security must lie in the choice of the key.--can be expanded on.

Kermit—A (once) popular file transfer and terminal emulation program.

Key (cryptovariable)—In cryptography, a sequence of symbols that controls encryption and decryption. For some encryption mechanisms (symmetric), the same key is used for both encryption and decryption; for other mechanisms (asymmetric), the keys used for encryption and decryption are different.

Key fingerprint—The actual binary code of an encryption key, which is presented in hexadecimal notation.

Key generation—The origination of a key or set of distinct keys.

Key length—The number of binary digits, or bits, in an encryption algorithm's key. Key length is sometimes used to measure the relative strength of the encryption algorithm.

Key logger (or key trapper) software—A program that, when installed on a computer, records every keystroke and mouse click.

Key management—The generation, storage, distribution, deletion, archiving and application of keys in accordance with a security policy.

Key space—The total number of possible values of keys in a cryptographic algorithm or other security measure such as a password. For example, a 20 bit key would have a key space of 1,048,576. See *key length* and *key fingerprint.*

Key, primary—A unique attribute used to identify a class of records in a database.

Key2audio—A product of Sony designed to control the copying of CDs by embedding code within the CD that prevents playback on a PC or Mac preventing track ripping or copying.

Keyboard—Today's most popular input technology.

Key-to-disk device—A keyboard unit that records data as patterns of magnetic spots onto magnetic disks.

Kilobyte (K byte)—The equivalent of 1,204 bytes.

KMI—Key management infrastructure.

Knowledge—Information from multiple sources integrated with common, environmental, real-world experience.

Knowledge acquisition—The component of the expert system that the knowledge engineer uses to enter the rules.

Knowledge base—The part of an expert system that contains specific information and facts about the expert area. Rules that the expert system uses to make decisions are derived from this source.

Knowledge engineer—The person who formulates the domain expertise of an expert system.

Knowledge levels—Verbs that describe actions an individual should be capable of performing on the job after completion of the training associated with the cell. The verbs are identified for three training levels: Beginning, Intermediate, and Advanced.

Knowledge worker—Works with and produces information as a product.

Knowledge-based system—An artificial intelligence system that applies reasoning capabilities to reach a conclusion. Also known as an expert system.

Known-cover attack—A type of attack where both the original, unaltered cover and the stego-object are available.

Known-message attack—A type of attack where the hidden message is known to exist by the attacker and the stego-object is analyzed for patterns which may be beneficial in future attacks. This is a very difficult attack, equal in difficulty to a stego-only attack.

Known-stego attack—An attack where the tool (algorithm) is known and the original cover object and stego-object are available.

L2F Protocol—Layer 2 Forwarding Protocol. Protocol that supports the creation of secure virtual private dial-up networks over the Internet.

Label—A set of symbols used to identify or describe an item, record, message, or file.

LAN—Local Area Network. High-speed, low-error data network covering a relatively small geographic area (up to a few thousand meters). LANs connect workstations, peripherals, terminals, and other devices in a single building or other geographically limited area. LAN standards specify cabling and signaling at the physical and data-link layers of the OSI model. Ethernet, FDDI, and Token Ring are widely used LAN technologies. *Compare with* MAN and WAN.

LAN Switch—High-speed switch that forwards packets between data-link segments. Most LAN switches forward traffic based on MAC addresses. This variety of LAN switch is sometimes called a frame switch. LAN switches are often categorized according to the method they use to forward traffic: cut-through packet switching or store-and-forward packet switching. Multi-layer switches are an intelligent subset of LAN switches. *Compare with* multi-layer switch. *See also* cutthrough packet switching and store-and-forward packet switching.

Language processing—The step of ASR in which the system attempts to analyze and make sense of the user's verbal instructions by comparing the word phonemes generated in step 2 with a language model database.

Language Translator—Systems software that converts programs written in assembler or a higher-level language into machine code.

LAPB—Link Access Procedure — Balanced.

LAPD—Link Access Procedure on the D Channel.

LAPF—Link Access Procedure for Frame-Mode Bearer Services.

Laser—Light Amplification by Stimulated Emission of Radiation. Analog transmission device in which a suitable active material is excited by an external stimulus to produce a narrow beam of coherent light that can be modulated into pulses to carry data. Networks based on laser technology are sometimes run over SONET.

Laser Printer—An output unit that uses intensified light beams to form an image on an electrically charged drum and then transfers the image to paper.

Last mile bottleneck problem—Occurs when information is traveling on the Internet over a very fast line for a certain distance and then comes near the user where it must travel over a slower line.

LAT—Local area transport.

Latency—In local networking, the time (measured in bits at the transmission rate) for a signal to propagate around or throughput the network. The time taken by a DASD device to position a storage location to reach the read arm over the physical storage medium. For general purposes, average latency time is used. Delay between the time a device requests access to a network and the time it is granted permission to transmit.

Law Enforcement Agency (LEA)—Organization authorized by a lawful authorization based on a national law to receive the results of telecommunications interceptions.

Law Enforcement Monitoring Facility (LEMF)—Law enforcement facility designated as the transmission destination for the results of interception relating to a particular interception subject.

Law Enforcement Official—See Part II, 45 CFR 164.501.

Lawful authorization—Permission granted to an LEA under certain conditions to intercept specified telecommunications and requiring cooperation from an NWO/AP/SvP. Typically, this refers to a warrant or order issued by a lawfully authorized body.

Lawful interception or intercept—See Interception.

Laws and regulations—Federal, government-wide and organization-specific laws, regulations, policies, guidelines, standards, and procedures mandating requirements for the management and protection of information technology resources.

Layer 3 Switching—The emerging layer 3 switching technology integrates routing with switching to yield very high routing throughput rates in the millions-of-packets-per-second range. The movement to layer 3 switching is designed to address the downsides of the current generation of layer 2 switches, which are functionally equivalent to bridges. These downsides for a large, flat network include being subject to broadcast storms, spanning tree loops, and address limitations that drove the injection of routers into bridged networks in the late 1980s. Currently, layer 3 switching is represented by a number of approaches in the industry.

Layered Defense—A combination of security services, software and hardware, infrastructures, and processes which are implemented to achieve a required level of protection. These mechanisms are additive in nature with the minimum protection being provided by the network and infrastructure layers.

LCD—Lifecycle support, lifecycle definition.

LCN—Logical Channel Number (X.25).

LCP—Link Control Protocol (X.25).

LDAP—Lightweight Directory Access Protocol. Protocol that provides access for management and browser applications that provide read/write interactive access to the X.500 Directory.

LDN—Local dial number (ISDN).

Learning—Knowledge gained by study (in classes or through individual research and investigation).

Learning continuum—A representation in which the common characteristic of learning is presented as a series of variations from awareness through training to education.

Learning objective—A link between the verbs from the “knowledge levels” section to the “Behavioral Outcomes” by providing examples of the activities an individual should be capable of doing after successful completion of training associated with the cell. Learning Objectives recognize that training must be provided at Beginning, Intermediate, and Advanced levels.

Leased Line—An un-switched telecommunications channel leased to an organization for its exclusive use.

Least Cost Routing (LCR)—The automatic selection of the most economically available route for each outgoing trunk call. Also known as automatic route selection.

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.).

Least Recently Used (LRU)—A replacement strategy in which new data must replace existing data in an area of storage; the least recently used items are replaced.

Least significant bit steganography—A substitution method of steganography where the right most bit in a binary notation is replaced with a bit from the embedded message. This method provides "security through obscurity", a technique which can be rendered useless if an attacker knows the technique is being used. .

Legacy Information System—An operational IS that existed prior to the implementation of the DITSCAP.

Legacy system—A previously built system using older technologies such as mainframe computers and programming languages such as COBOL.

Letter bomb—A Trojan horse that triggers 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.

Lightweight Directory Access Protocol (LDAP)—This protocol provides access for management and browser application that provide read/write interactive access to the X.500 Directory.

Likert scale—an evaluation tool that is usually from one to five (one being very good; five being not good, or vice versa), designed to allow an evaluator to prioritize the results of the evaluation.

Limit check—An input control text that assesses the value of a data field to determine whether values fall within set limits.

Line conditioning—A service offered by common carriers to reduce delay, noise, and amplitude distortion to produce transmission of higher data speeds.

Line printer—An output unit that prints alphanumeric characters one line at a time.

Line speed—The transmission rate of signals over a circuit, usually expressed in bits per second.

Line-of-Sight (LOS)—Defined by the Fresnel Zone. Fresnel zone clearance is the minimum clearance over obstacles that the signal needs to be sent over. Reflection or path bending occurs if the clearance is not sufficient.

Linguistic steganography—The method of steganography where a secret is embedded in a harmless message. See also *Jargon Code*.

Link encryption—The application of online crypto-operations to a link of a communications system so that all information passing over the link is encrypted in its entirety.

Linkage—The purposeful combination of data or information from one information system with that from another system in the hope of deriving additional information.

Linux—An open source operating system that provides a rich operating environment for high-end workstations and network servers.

List—A collection of information arranged in columns and rows in which each column displays one particular type of information.

List definition table—A description of a list by column.

LLC—Logical Link Control.

LLD—Development, low-level design.

LMI—Local Management Interface (Frame Relay).

Load Sharing—A multiple-computer system that shares the load during peak hours. During non-peak periods or standard operation, one system can handle the entire load with the others acting as fallback units.

Local Area Network (LAN)—The physical connection of microcomputers with communication media (e.g., cable and fiber optics) that allows the sharing of information and peripherals among those microcomputers.

Local code(s)—A generic term for code values that are defined for a state or other political subdivision, or for a specific payer. This term is most commonly used to describe HCPCS Level III Codes, but also applies to state-assigned Institutional Revenue Codes, Condition Codes, Occurrence Codes, Value Codes, etc.

Local loop—The physical connection from the subscriber's premises to the carrier's point of presence (POP). The local loop can be provided over any suitable transmission medium.

Local Multipoint Distribution Services (LMDS)—A method of distributing TV signals to households in a local community. LMDS uses broadcast microwave signals to contact local dishes. The received signal is then distributed through the central CATV system.

Location information—Information relating to the geographical, physical, or logical location of an identity relating to an interception subject.

Lock/key protection system—A protection system that involves matching a key or a password with a specified access requirement.

Logged-on but Unattended—A workstation is considered logged on but unattended when the user is (1) Logged on but is not physically present in the office; and (2) There is no one else present with an appropriate level of clearance safeguarding access to the workstation. Coverage must be equivalent to that which would be required to safeguard hard copy information if the same employee were away from his or her desk. Users of logged on but unattended classified workstations are subject to the issuance of security violations.

Logging—The automatic recording of data for the purpose of accessing and updating it.

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

Logical error—A programming error that causes the wrong processing to take place in a syntactically valid program.

Logical file organization—The sequencing of data records in a file according to their key.

Logical Link Control (LLC)—The portion of the link level protocol in the 802 standards that is in direct contact with higher-level layers.

Logical Observation Identifiers, Names and Codes (LOINC)—A set of universal names and ID codes that identify laboratory and clinical observations. These codes, which are maintained by the Regenstrief Institute, are expected to be used in the HIPAA claim attachments standard.

Logical operation—A comparison of data values within the arithmetic logic unit. These comparisons show when one value is greater than, equal to, or less than a second value.

Logical operator—A symbol used in programming that initiates a comparison operation of two or more data values.

Logical organization—Data elements organized in a manner that meets human and organizational processing needs.

Logically disconnect—Although the physical connection between the control unit and a terminal remains intact, a system enforced disconnection prevents communication between the control unit and the terminal.

LOINC—See Logical Observation Identifiers, Names and Codes.

Loop—A repeating structure or process.

Loophole—An error of omission or oversight in software, hardware, or firmware that permits circumventing the access control process.

Lost Pouch—Any pouch-out-of-control which is not recovered.

LRA—Local registration authority (for digital certificates).

LSA—Link-state advertisement.

LSP—Link state packet.

LT—Local termination.

LTC—Long-Term Care.

M+CO—Medicare Plus Choice Organization.

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

MAC (1)—Mandatory Access Control.

MAC (2)—Message Authentication Code.

MAC (3)—Media Access Control.

MAC (Media Access Control)—See *media access control.* .

MAC Address—Standardized data-link layer address ingrained into a NIC that is required for every port or device that connects to a LAN. Other devices in the network use these addresses to locate specific ports in the network and to create and update routing tables and data structures. MAC addresses are 6 bytes long and are controlled by the IEEE. Also known as a hardware address, MAC-layer address, and physical address. *Compare with* network address.

Mac OS—The operating system for today's apple computers.

Machine Language—Computer instructions or code representing computer operations and memory addresses in a numeric form that is executable by the computer without translation.

Machine language—Computer instructions or code representing computer operations and memory addresses in a numeric form that is executable by the computer without translation.

Macro viru—A computer virus that spreads by binding itself to software such as Word or Excel.

Madison Project—A code name for IBM's Electronic Music Management System (EMMS). EMMS is being designed to deliver piracy-proof music to consumers via the Internet.

Magicgate—A memory media stick from Sony designed to allow users access to copyrighted music or data.

Magnetic disk—A storage device consisting of metallic platters coated with an oxide substance that allows data to be recorded as patterns of magnetic spots.

Magnetic Ink Character Recognition (MICR)—An input method under which data is encoded in special ink containing iron particles. These particles can be magnetized and sensed by special machines and converted into computer input.

Magnetic tape—A storage medium consisting of a continuous strip of coated plastic film wound onto a reel and on which data can be recorded as defined patterns of magnetic spots.

Mail gateway—A machine that connects two or more e-mail systems (especially dissimilar mail systems on two different networks) and transfers messages between them. Sometimes the mapping and translation can be quite complex, and generally it requires a store-and-forward scheme whereby the message is received from one system completely before it is transmitted to the next system after suitable translations.

Mail relay server—An e-mail server that relays messages where neither the sender nor the receiver is a local user. A risk exists that an unauthorized user could hijack these open relays and use them to spoof their own identity.

Mail server—Provides e-mail services and accounts.

Mailing list—Discussion groups organized by area of interest.

Mainframe computer—A computer designed to meet the computing needs of hundreds of people in a large business environment.

Maintain or Maintenance—See Part II, 45 CFR 162.103.

Maintainability—The general ease of a system to be maintained, at all levels of maintenance.

Maintenance—Tasks associated with the modification or enhancement of production software.

Maintenance Organization—The government organization responsible for the maintenance of an IS. (Although the actual organization performing maintenance on a system may be a contractor, the maintenance organization is the government organization responsible for the maintenance.).

Maintenance phase—Monitors and supports the new system to ensure it continues to meet the business goals.

Maintenance Programmer—An applications programmer responsible for making authorized changes to one or more computer programs and ensuring that the changes are tested, documented, and verified.

Major application—An application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to, or modification of, the information in the application. A breach in a major application might comprise many individual application programs and hardware, software, and telecommunications components. Major applications can be either major software applications or a combination of hardware/software where the only purpose of the system is to support a specific mission-related function.

MAN—Metropolitan area network.

Management controls—Actions taken to manage the development, maintenance, and use of the system, including system-specific policies, procedures, and rules of behavior, individual roles and responsibilities, individual accountability, and personnel security decisions.

Management Information Systems (MIS)—Deals with the planning, development, management, and use of information technology tools to help people perform tasks related to information processing and management.

Mandatory Access Control (MAC)—MAC is a means of restricting access to data based on varying degrees of security requirements for information contained in the objects.

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.

MAP—Manufacturing Automation Protocol.

Maritime Strategy—Naval objectives for sea control, maritime power projection, and control and protection of shipping. The Naval objectives in support of the National Strategy.

Marketing—See Part II, 45 CFR 164.501.

Marketing mix—The set of marketing tools that a firm uses to pursue its marketing objectives in the target market.

Masquerade—A type of security threat that occurs when an entity successfully pretends to be a different entity.

Mass customization—When a business gives its customers the opportunity to tailor its product or service to the customer’s specifications.

Massachusetts Health Data Consortium (MHDC)—An organization that seeks to improve healthcare in New England through improved policy development, better technology planning and implementation, and more informed financial decision making.

Master file—An automated file that contains semi-permanent or permanent information and is maintained over a time period required by organizational policy.

Master plan—A long-range plan, derived from the notional architecture, for development and procurement of capabilities.

Matrix display—The alphanumeric representation of characters as patterns of tiny dots in specific positions on a display terminal.

Matrix printer—A hard-copy printing device that forms alphanumeric characters with small pins arranged in a matrix of rows and columns.

Mature system—A fully operational system that performs all the functions it was designed to accomplish.

MAU—Media Attachment Unit.

Maximum Defined Data Set—Under HIPAA, this is all of the required data elements for a particular standard based on a specific implementation specification. An entity creating a transaction is free to include whatever data any receiver might want or need. The recipient is free to ignore any portion of the data that is not needed to conduct their part of the associated business transaction, unless the inessential data is needed for coordination of benefits. Also see Part II, 45 CFR 162.103.

MCO—Managed Care Organization.

M-commerce—The term used to describe E-commerce conducted over a wireless device such as a cell phone or personal digital assistant.

MCS—TOE access, limitation on multiple concurrent sessions.

MD5 hash value—A mathematically generated string of 32 letters and digits that is unique for an individual storage medium at a specific point in time.

MDx—Message Digest (e.g., MD5).

Media—The various physical forms (e.g., disk, tape, and diskette) on which data is recorded in machine-readable formats.

Media Access Control (MAC)—Lower of the two sub-layers of the data-link layer defined by the IEEE. The MAC sub-layer handles access to shared media, such as whether token passing or contention will be used. A local network control protocol that governs station access to a shared transmission medium. Examples are token passing and CSMA. See also *carrier sense, multiple access.*

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.

Mediation function—A mechanism that passes information between an NWO, an AP or an SvP, and a handover interface, and information between the internal network interface and the handover interface.

Medicaid Fiscal Agent (FA)—The organization responsible for administering claims for a state Medicaid program.

Medicaid State Agency—The state agency responsible for overseeing the state's Medicaid program.

Medical Code Sets—Codes that characterize a medical condition or treatment. These code sets are usually maintained by professional societies and public health organizations. Compare to administrative code sets.

Medical Records Institute (MRI)—An organization that promotes the development and acceptance of electronic healthcare record systems.

Medicare Contractor—A Medicare Part A Fiscal Intermediary, a Medicare Part B Carrier, or a Medicare Durable Medical Equipment Regional Carrier (DMERC).

Medicare Durable Medical Equipment Regional Carrier (DMERC)—A Medicare contractor responsible for administering Durable Medical Equipment (DME) benefits for a region.

Medicare Part A Fiscal Intermediary (FI)—A Medicare contractor that administers the Medicare Part A (institutional) benefits for a given region.

Medicare Part B Carrier—A Medicare contractor that administers the Medicare Part B (Professional) benefits for a given region.

Medicare Remittance Advice Remark Codes—A national administrative code set for providing either claim-level or service-level Medicare-related messages that cannot be expressed with a Claim Adjustment Reason Code. This code set is used in the X12 835 Claim Payment & Remittance Advice transaction, and is maintained by the HCFA.

Megabyte (Mbyte, MB)—The equivalent of 1,048,576 bytes.

Megahertz (MHz)—The number of millions of CPU cycles per second.

Memorandum of Understanding (MOU)—A document that provides a general description of the responsibilities that are to be assumed by two or more parties in their pursuit of some goal(s). More specific information may be provided in an associated SOW.

Memorandum of understanding/agreement—A document established between two or more parties to define their respective responsibilities in accomplishing a particular goal or mission. In this guide, an MOU/A defines the responsibilities of two or more organizations in establishing, operating, and securing a system interconnection. .

Memory—The area in a computer that serves as temporary storage for programs and data during program execution.

Memory address—The location of a byte or word of storage in computer memory.

Memory bounds—The limits in the range of storage addresses for a protected region in memory.

Memory chips—A small integrated circuit chip with a semiconductor matrix used as computer memory.

Menu—A section of the computer program--usually the top-level module--that controls the order of execution of other program modules. Also, online options displayed to a user, prompting the user for specific input.

Message—1. The data input by the user in the online environment that is used to drive a transaction. The output of transaction. 2. In steganography, the data a sender wishes to remain confidential. This data can be text, still images, audio, video or anything that can be represented as a bitstream.

Message address—The information contained in the message header that indicates the destination of the message.

Message Authentication Code (MAC)—Message Authentication Code is a one-way hash computed from a message and some secret data. It is difficult to forge without knowing the secret data. Its purpose is to detect if the message has been altered.

Message digest—An example would be MD5. A message digest is a combination of alphanumeric characters generated by an algorithm that takes a digital object (such as a message you type) and pulls it through a mathematical process, giving a digital fingerprint of the message (enabling you to verify the integrity of a given message).

Message Handling System (MHS)—The system of message user agents, message transfer agents, message stores, and access units that together provide OSI e-mail. MHS is specified in the ITU-TSS X.400 series of recommendations.

Message Stream—The sequence of messages or parts of messages to be sent.

Message Transfer Agent (MTA)—An OSI application process used to store and forward messages in the X.400 message handling system. Equivalent to Internet mail agent.

Messaging application—An application based on a store and forward paradigm; it requires an appropriate security context to be bound with the message itself.

Messaging service—An interactive service that offers user-to-user communication between individual users via storage units with store-and-forward, and mailbox or message handling functions (e.g., information editing, processing, and conversion).

Messaging-based workflow system—Sends work assignments through an e-mail system.

Metadata—The description of such things as the structure, content, keys, and indexes of data.

Metalanguage—A language used to specify other languages.

Metatag—A part of a Web site text not displayed to users but accessible to browsers and search engines for finding and categorizing Web sites.

Method—A function, capability, algorithm, formula, or process that an object is capable of performing.

Metropolitan Area Network (MAN)—A data network intended to serve an area approximating that of a large city. Such networks are being implemented by innovative techniques, such as running fiber cables through subway tunnels.

MGMA—Medical Group Management Association.

MHDC—See the Massachusetts Health Data Consortium.

MHDI—See the Minnesota Health Data Institute.

MIB—Management information base.

Microcomputer—A small microprocessor-based computer built to handle input, output, processing, and storage functions.

Microdot—a detailed form of microfilm that has been reduced to an extremely small size for ease of transport and purposes of security.

Microfilm—A film for recording alphanumeric and graphics output that has been greatly reduced in size.

Micro-payment—A technique to facilitate the exchange of small amounts of money for an Internet transaction.

Microphone—For capturing live sounds, such as human voice.

Microprocessor—A single small chip containing circuitry and components for arithmetic, logical, and control operations.

Microsoft Windows 2000 Millennium (Windows 2000Me)—An operating system for a home computer featuring utilities for setting up a home network and performing video, photo, and music editing and cataloging.

Microsoft Windows 2000 Professional (Windows 2000 Pro)—An operating system for people who have a personal computer connected to a network of other computers at work or at school.

Microsoft Windows XP Home—Microsoft's latest upgrade to Windows 2000Me, with enhanced features for allowing multiple users to use the same computer.

Microsoft Windows XP Professional (Windows XP Pro) —Microsoft's latest upgrade to Windows 2000 Pro.

Microwave—A type of radio transmission used to transmit information.

Middleware—The distributed software needed to support interactions between client and servers.

MIDI—Musical instrument digital interface.

Millions of Instructions Per Second (MIPS)—Used as a measure for assessing the speed of mainframe computers. Also, meaningless indicator of processor speed.

Minicomputer—Typically, a word-oriented computer whose memory size and processing speed falls between that of a microcomputer and a medium-sized computer.

Minimum level of protection—The reduction in the total risk that results from the impact of in-place safeguards. See also *total risk, acceptable risk,* and *residual risk.*

Minimum Scope of Disclosure—The principle that, to the extent practical, individually identifiable health information should only be disclosed to the extent needed to support the purpose of the disclosure.

Minimum security baseline—A set of minimum acceptable security controls, which are applicable to a range of information technology systems.

Minimum security baseline assessment—An evaluation of controls protecting an information system against a set of minimum acceptable security requirements.

Minnesota Health Data Institute (MHDI)—A public-private partnership for improving the quality and efficiency of healthcare in Minnesota. MHDI includes the Minnesota Center for Healthcare Electronic Commerce (MCHEC), which supports the adoption of standards for electronic commerce and also supports the Minnesota EDI Healthcare Users Group (MEHUG).

Minor application—An application, other than a major application, that requires attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Minor applications are typically included as part of a general support system. .

MIPS—See *millions of instructions per second.*

Mirror Image Backup—Mirror image backups (also referred to as bitstream backups) involve the backup of all areas of a computer hard disk drive or another type of storage media (e.g., Zip disks, floppy disks, Jazz disks, etc.). Such mirror image backups exactly replicate all sectors on a given storage device. Thus, all files and ambient data storage areas are copied. Such backups are sometimes referred to as "evidence-grade" backups and they differ substantially from standard file backups and network server backups. The making of a mirror image backup is simple in theory, but the accuracy of the backup must meet evidence standards. Accuracy is essential and to guarantee accuracy, mirror image backup programs typically rely on mathematical CRC computations in the validation process. These mathematical validation processes compare the original source data with the restored data. When computer evidence is involved, accuracy is extremely important, and the making of a mirror image backup is typically described as the preservation of the "electronic crime scene.".

Mirrored site—An alternate site that contains the same information as the original. Mirror sites are set up for backup and disaster recovery as well to balance the traffic load for numerous download requests. Such "download mirrors" are often placed in different locations throughout the Internet.

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. 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.

Mission—A specific task with which a person, or group of individuals, or organization is entrusted to perform.

Mission criticality—The property that data, resources, and processes may have, which denotes that the importance of that item to the accomplishment of the mission is sufficient to be considered an enabling/disabling factor.

Mission justification—The description of the operational capabilities required to perform an assigned mission. This includes a description of a system's capabilities, functions, interfaces, information processed, operational organizations supported, and the intended operational environment.

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

Mjuice—An online music store that provides secure distribution of MP3s over the Internet. A secure player and a download system allow users to play songs an unlimited number of times, but only on a registered player.

MLP—Multi-link PPP.

MLS—Multi-level secure.

MMP—Multi-chassis Multi-link PPP.

MNWF—Must not work function.

Mobile Base Stations (MBS)—Component of cellular network that provides data link relay functions for a set of radio channels serving a cell.

Mobile site—The use of a mobile/temporary facility to serve as a business resumption location. They usually can be delivered to any site and can house information technology and staff.

Mobile Switching Center (MSC)—The location of the digital access and crossconnect system (DACS) in a cellular telephone network.

Mobile Telephone Switching Office (MTSO)—Controls the entire operation of a cellular system. It is a sophisticated computer that monitors all cellular calls, arranges handoffs and manages billing information.

Mode of Operation—A classification for systems that execute in a similar fashion and share distinctive operational characteristics (e.g., Production, DSS, online, and Interactive).

Model—A representation of a problem or subject area that uses abstraction to express concepts.

Model management—Component of a DSS that consists of the DSS models and the DSS model management system.

Modeling—The activity of drawing a graphical representation of a design.

Modem (Modulator/Demodulator)—Modulator/demodulator. This is a piece of hardware used to connect computers (or certain other network devices) together via a serial cable (usually a telephone line). When data is sent from your computer, the modem takes the digital data and converts it to an analog signal (the modulator portion). When you receive data into your computer via modem, the modem takes the analog signal and converts it to a digital signal that your computer will understand (the demodulator portion).

Modification—A type of security threat that occurs when its content is modified in an unanticipated manner by a non-authorized entity.

Modify or Modification—Under HIPAA, this is a change adopted by the secretary, through regulation, to a standard or an implementation specification. Also see Part II, 45 CFR 160.103.

Modular Treated Conference Room (MTCR)—A second-generation design of the treated conference room (TCR), offering more flexibility in configuration and ease of assembly than the original TCR, designed to provide acoustic and RF emanations protection.

Modularity—Modular packages consist of sets of equipment, people, and software tailorable for a wide range of missions.

MOF—Security management, management of functions in TSF.

Molecules—The smallest particle of a substance that retains all the properties of the substance and is composed of one or more atoms.

Monitoring and surveillance agents (or predictive agents)—Intelligent agents that observe and report on equipment.

Monitoring policy—The rules outlining the way in which information is captured and interpreted.

MOP—Maintenance Operation Protocol.

More stringent—See Part II, 45 CFR 160.202.

Mosaic attack—A watermarking attack that is particularly useful for images that are distributed over the Internet. It relies on a web browsers ability to assemble mutiple images so they appear to be one image. A watermarked image can be broken into pieces but displayed as a single image by the browser. Any program trying to detect the watermark will look at each individual piece, and if they are small enough, will not be able to detect the watermark.

MOU—See Memorandum of Understanding.

Mouse—A hardware device used for moving a display screen cursor.

MP—Multi-link Protocol.

MPEG—Motion Picture Experts Group.

MPR—Multi-protocol PC-based routing.

MR—Medical Review.

MRI—See the Medical Records Institute.

MRRU—Maximum Received Reconstructed Unit (PPP).

MSA—Security management, management of security attributes.

MSAU—Multi-station Access Units (Token Ring).

MSP—Medicare Secondary Payer.

MSU—Vulnerability assessment, misuse.

MTD—Security management, management of TSF data.

M-trax—An encrypted form of MP3 watermarking technology from MCY Music that protects the music industry and artists from copyright infringments.

MTU—Maximum transmission unit.

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

Multichannel Multipoint Distribution Services (MMDS)—An FCC name for a service where multiple video channels are broadcast within a limited geographic area. Often called wireless cable.

Multidimensional Analysis (MDA) tools—Slice and dice techniques that allow viewing multidimensional information from different perspectives.

Multifunction printer—Scans, copies, and faxes as well as prints.

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: (1) Some users do not have a valid security clearance for all the information processed in the IS; (2) all users have the proper security clearance and appropriate formal access approval for that information to which they have access; and (3) all users have a valid need-to-know only for information for which they have access.

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.

Multilevel Security (MLS)—Concept of processing information with different classifications and categories that simultaneously permits access by users with different security clearances, but prevents users from obtaining access to information for which they lack authorization.

Multinational Operations—A collective term to describe military actions conducted by forces of two or more nations usually undertaken within the structure of a coalition or alliance.

Multiple inheritance—The language mechanism that allows the definition of a class to include the attributes and methods defined for more than one superclass.

Multiplexing—To transmit two or more signals over a single channel.

Multiprocessing—A computer operating method in which two or more processors are linked and execute multiple programs simultaneously.

Multiprogramming—A computer operating environment in which several programs can be placed in memory and executed concurrently.

Multi-purpose Internet Mail Extension (MIME)—The standard for multimedia mail contents in the Internet suite of protocols.

Multitasking—Allows the user to work with more than one piece of software at a time.

Municipal area network (MAN)—A network that covers a metropolitan area.

MUSE project—An initiative which contributes to the continuing development of intellectual property standards. The MUSE project focuses on the electronic delivery of media, embedded signaling systems, and encryption technology with the goal of creating a global standard.

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.

Mutation—The process within a genetic algorithm of randomly trying combinations and evaluating the success or failure of the outcome.

Mutually suspicious—Pertaining to a state that exists between interactive processes (systems or programs), each of which contains sensitive data and is assumed to be designed to extract data from the other and to protect its own data.

MW—Multi-channel interface proccessor.

MWF—Must work function.

NAHDO—See the National Association of Health Data Organizations.

NAIC—See the National Association of Insurance Commissioners.

NAK—Negative acknowledgment. Response sent from a receiving device to a sending device indicating that the information received contained errors. Compare with *acknowledgment.*

NAK Attack—A penetration technique that capitalizes on an operating system's inability to properly handle asynchronous interrupts.

Name Resolution—The process of mapping a name into the corresponding address.

Naming Attributes—Names carried by each instance of an object, such as name, or identification number.

NASMD—See the National Association of State Medicaid Directors.

NAT—Network Address Translation. A means of hiding the IP addresses on an internal network from external view. NAT boxes allow net managers to use any IP addresses they choose on internal networks, thereby helping to ease the IP addressing crunch while hiding machines from attackers.

National Association of Health Data Organizations (NAHDO)—A group that promotes the development and improvement of state and national health information systems.

National Association of Insurance Commissioners (NAIC)—An association of the insurance commissioners of the states and territories.

National Association of State Medicaid Directors (NASMD)—An association of state Medicaid directors. NASMD is affiliated with the American Public Health Human Services Association (APHSA).

National Center for Health Statistics (NCHS)—A federal organization within the CDC that collects, analyzes, and distributes healthcare statistics. The NCHS maintains the ICD-n-CM codes.

National Committee for Quality Assurance (NCQA)—An organization that accredits managed care plans, or Health Maintenance Organizations (HMOs). In the future, the NCQA may play a role in certifying these organizations' compliance with the HIPAA A/S requirements. The NCQA also maintains the Health Employer Data and Information Set (HEDIS).

National Committee on Vital and Health Statistics (NCVHS)—A federal advisory body within HHS that advises the secretary regarding potential changes to the HIPAA standards.

National Computer Security Center (NCSC)—Originally named the DoD Computer Security Center, the NCSC is responsible for encouraging the widespread availability of trusted computer systems throughout the federal government. With the signing of NSDD-145; the NCSC is responsible for encouraging the widespread availability of trusted computer systems throughout the federal government.

National Council for Prescription Drug Programs (NCPDP)—An ANSI-accredited group that maintains a number of standard formats for use by the retail pharmacy industry, some of which are included in the HIPAA mandates. Also see *NCPDP . . . Standard.*

National Drug Code (NDC)— A medical code set that identifies prescription drugs and some over-the-counter products, and that has been selected for use in the HIPAA transactions.

National Employer ID— A system for uniquely identifying all sponsors of healthcare benefits.

National Health Information Infrastructure (NHII)—This is a healthcare-specific lane on the information superhighway, as described in the National Information Infrastructure (NII) initiative. Conceptually, this includes the HIPAA A/S initiatives.

National Information Assurance Partnership (NIAP)—A joint industry/government initiative, lead by NIST and NSA, to establish commercial testing laboratories where industry product providers can have security products tested to verify their performance against vendor claims.

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.

National Patient ID—A system for uniquely identifying all recipients of healthcare services. This is sometimes referred to as the National Individual Identifier (NII), or as the Healthcare ID.

National Payer ID—A system for uniquely identifying all organizations that pay for healthcare services. Also known as Health Plan ID or Plan ID.

National Provider File (NPF)—The database envisioned for use in maintaining a national provider registry.

National Provider ID (NPI)—A system for uniquely identifying all providers of healthcare services, supplies, and equipment.

National Provider Registry—The organization envisioned for assigning National Provider IDs.

National Provider System (NPS)—The administrative system envisioned for supporting a national provider registry.

National Science Foundation (NSF)—Sponsors of the NSFNET.

National Science Foundation Network (NSFNET)—A collection of local, regional, and mid-level networks in the U.S. tied together by a high-speed backbone. NSFNET provides scientists access to a number of supercomputers across the country.

National Security—The national defense or foreign relations of the United States.

National security information—Information that has been determined pursuant to Executive Order 12958 as amended by Executive Order 13292, 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. .

National security system—Any information system (including any telecommunications system) used or operated by an organization or by a contractor of the organization, or by other organization on behalf of the organization: (1) the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions (excluding a system that is to be used for routine administrative and business applications, for example, payroll, finance, logistics, and personnel management applications); or (2) is protected at all times by procedures established for information that have 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. .

National Standard Format (NSF)—Generically, this applies to any nationally standardized data format, but it is often used in a more limited way to designate the Professional EMC NSF, a 320-byte flat file record format used to submit professional claims.

National strategy—Objectives of the nation for dealing in the arena of international politics, military confrontation, and national defense.

National Uniform Billing Committee (NUBC)—An organization, chaired and hosted by the American Hospital Association, that maintains the UB-92 hardcopy institutional billing form and the data element specifications for both the hardcopy form and the 192-byte UB-92 flat file EMC format. The NUBC has a formal consultative role under HIPAA for all transactions affecting institutional healthcare services.

National Uniform Claim Committee (NUCC)—An organization, chaired and hosted by the American Medical Association, that maintains the HCFA-1500 claim form and a set of data element specifications for professional claims submission via the HCFA-1500 claim form, the Professional EMC NSF, and the X12 837. The NUCC also maintains the Provider Taxonomy Codes and has a formal consultative role under HIPAA for all transactions affecting non-dental non-institutional professional healthcare services.

Natural language—A language that is used in communication with computers and that closely resembles English syntax.

NAUN—Nearest active upstream neighbor.

NBMA—Nonbroadcast multi access.

NBP—Name Binding Protocol (AppleTalk).

NCHICA—See the North Carolina Healthcare Information and Communications Alliance.

NCHS—See the National Center for Health Statistics.

NCP—NetWare Core Protocol.

NCP—Network Control Protocol (PPP).

NCPDP—See the National Council for Prescription Drug Programs.

NCPDP Batch Standard—An NCPDP standard designed for use by low-volume dispensers of pharmaceuticals, such as nursing homes. Use of Version 1.0 of this standard has been mandated under HIPAA.

NCPDP Telecommunication Standard—An NCPDP standard designed for use by high-volume dispensers of pharmaceuticals, such as retail pharmacies. Use of Version 5.1 of this standard has been mandated under HIPAA.

NCQA—See the National Committee for Quality Assurance.

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

NCVHS—See the National Committee on Vital and Health Statistics.

NDC— See National Drug Code.

NDIS—Network Driver Interface Specification.

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.

Negative Acknowledgment (NAK)—A response sent by the receiver to indicate that the previous block was unacceptable and the receiver is ready to accept a retransmission.

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.

NetBIOS—Network Basic I/O System.

Network—An integrated, communicating aggregation of computers and peripherals linked through communications facilities.

Network Access Layer—The layer of the TCP/IP stack that sends the message out through the physical network onto the Internet.

Network Access Points (NAPs)—(1) Nodes providing entry to the highspeed Internet backbone system. (2) Another name for an Internet Exchange Point.

Network Address—The network portion of an IP address. For a class A network, the network address is the first byte of the IP address. For a class B network, the network address is the first two bytes of the IP address. For a class C network, the network address is the first three bytes of the IP address. In the Internet, assigned network addresses are globally unique.

Network Administrator—The person who maintains user accounts, password files, and system software on your campus network.

Network Basic Input Output System (NetBIOS)—The standard interface to networks on IBM PC and compatible system.

Network centric—A holistic view of interconnected information systems and resources that encourages a broader approach to security management than a component-based approach.

Network element—A component of the network structure such as a local exchange, higher-order switch, or service-control processor.

Network File Systems (NFS)—A distributed file system developed by Sun Microsystems which allows a set of computers to cooperatively access each other's files in a transparent manner.

Network hub—A device that connects multiple computers into a network.

Network Information Center (NIC)—Originally, there was only one, located at SRI International and tasked to serve the ARPANET (and later DDN) community. Today, there are many NICs, operated by local, regional, and national networks all over the world. Such centers provided user assistance, document service, training, and much more.

Network layer—The OSI layer that is responsible for routing, switching, and subnetwork access across the entire OSI environment. Think of this layer as a post office that delivers letters based on the address written on an envelope.

Network manager—Provides a package of end-user functions with the responsibility for the management of a network, mainly as supported by the EMs, but it may also involve direct access to the network elements. All communication with the network is based on open and well-standardized interfaces supporting management of multivendor and multi-technology network elements.

Network Operator (NWO)—Operator of a public telecommunications infrastructure that permits the conveyance of signals between defined network termination points by wire, microwave, optical means, or other electromagnetic means.

Network propagation system analysis—a way of determining the speed and method of stego-object (or virus) movement throughout a network.

Network Service Provider (NSP)—Owns and maintains routing computers at NAPs and even the lines that connect the NAPs to each other. For example, MCI and AT&T.

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

Networking—A method of linking distributed data processing activities through communications facilities.

Networks—Includes communication capability that allows one user or system to connect to another user or system and can be part of a system or a separate system. Examples of networks include local area network or wide area networks, including public networks such as the Internet. .

Neural Network—A type of system developed by artificial intelligence researchers used for processing logic.

Newsgroups—Usually discussions, but not "interactively live." Newsgroups are like posting a message on a bulletin board and checking at various times to see if someone has responded to your posting.

Newspaper Code—a hidden communication technique where small holes are poked just above the letters in a newspaper article that will spell out a secret message. A variant of this technique is to use invisible ink place of holes.

NFS—Network file system.

NHII—See National Health Information Infrastructure.

NIACAP—National Information Assurance Certification and Accreditation Process.

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

NIAP Common Criteria Evaluation and Validation Scheme—The scheme developed by NIST and NSA as part of the National Information Assurance Partnership (NIAP) establishing an organizational and technical framework to evaluate the trustworthiness of IT products.

NIAP Oversight Body—A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

NIC—Network Interface Card. This is the card that the network cable plugs into in the back of your computer system. The NIC connects your computer to the network. A host must have at least one NIC; however, it can have more than one. Every NIC is assigned a MAC address.

NIDS—Network intrusion detection system.

NII—National information infrastructure of a specific country.

NIPC—U.S. National Infrastructure Protection Center.

NIST—National Institute of Standards and Technology.

NLPID—Network Level Protocol Identifier.

NLS—Network Layer Security Protocol.

NLSP—NetWare Link Service Protocol.

NNI—Network to Network Interface (ATM, Frame Relay).

NOC—In HIPAA, Not Otherwise Classified or Nursing Outcomes Classification.

Node—A point of connection into a network. In multipoint networks, is a unit that is polled. In LANs, it is a device on the ring. In packet switched networks, it is one of the many packet switches that form the network's backbone.

NOI—See *notice of intent.*

Noise—Random electrical signals introduced by circuit components or natural disturbances that tend to degrade the performance of a communications channel.

Nonclinical or Nonmedical Code Sets—See *administrative code sets.*

Noncomputing Security Methods—Noncomputing methods are security safeguards which do not use the hardware, software, and firmware of the IS. Traditional methods include physical security (controlling physical access to computing resources), personnel security, and procedural security.

Nondevelopmental Item (NDI)—Any item that is available in the commercial marketplace; any previously developed item that is in use by a Department or Agency of the United States, a state or local government, or a foreign government with which the United States has a mutual defense cooperation agreement; any item described above that requires only minor modifications in order to meet the requirements of the procuring Agency; or any item that is currently being produced that does not meet the requirements of definitions above, solely because the item is not yet in use or is not yet available in the commercial marketplace.

Non-discretionary access control—A non-discretionary authorization scheme is one under which only the recognized security authority of the security domain may assign or modify the ACI for the authorization scheme such that the authorizations of principals under the scheme are modified.

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.

Non-intrusive monitoring—The use on non-intrusive probes or traces to assemble information and track traffic and identity vulnerabilities.

Nonprocedural language—A programming language with fixed logic, which allows the programmer to specify processing operations without concern for processing logic.

Nonrecord material—Extra and duplicate copies that are only of temporary value, including shorthand notes, used carbon paper, preliminary drafts, and other material of similar nature.

Nonrecurring (ad hoc) decision—One that is made infrequently and may have different criteria for determining the best solution each time.

Non-repudiation—A security service by which evidence is maintained so that the sender and recipient of data cannot deny having participated in the communication. Referred to individually as non-repudiation of origin and non-repudiation of receipt.

Nonstructured decision—A decision for which there may be several right answers and there is no precise way to get a right answer.

Nontransparent Proxy Mode Accelerator—In a Nontransparent Proxy Mode Accelerator, the source addresses of all the packets decrypted by the SSL accelerator have a source address of that SSL accelerator and the client source addresses do not get to the server at all. From the server perspective, the request has come from the SSL accelerator.

Normalization—A process of assuring that a relational database structure can be implemented as a series of two-dimensional relations.

North Carolina Healthcare Information and Communications Alliance (NCHICA)—An organization that promotes the advancement and integration of information technology into the healthcare industry.

NOS—Network operating system.

Notebook computer—A highly portable, battery powered microcomputer with a display screen, carried easily in a briefcase, and used away from a user's workplace.

Notice—A privacy principle that requires reasonable disclosure to a consumer of an entity's personally identifiable information (PII) collection and use practices. This disclosure information is typically conveyed in a privacy notice or privacy policy. Microsoft: http://www.microsoft.com/security/glossary/.

Notice of Intent (NOI)—A document that describes a subject area for which the federal government is considering developing regulations. It may describe the presumably relevant considerations and invite comments from interested parties. These comments can then be used in developing an NPRM or a final regulation.

Notice of Proposed Rulemaking (NPRM)—A document that describes and explains regulations that the federal government proposes to adopt at some future date, and invites interested parties to submit comments related to them. These comments can then be used in developing a final regulation.

Notional Architecture—An alternative architecture composed of current systems, as well as, new procurements proposed for some future date.

NPF—See *National Provider File.*

NPI—See *National Provider ID.*

NPRM—Notice of Proposed Rulemaking--the publication, in the *Federal Register*, of proposed regulations for public comment.

NPRM—See *Notice of Proposed Rulemaking.*

NPS—See *National Provider System.*

NRC—National Research Council--quasi-governmental body that conducted a study on the state of security in health care: *For the Record: Protecting Electronic Health Information* (Washington, DC: National Academy Press, 1997).

NRO—Communication non-repudiation of origin.

NRR—Communication non-repudiation of receipt.

NSF—See *National Standard Format.*

NT-1—Network Termination 1.

NTN—Network Terminal Number (X.25).

NTP—Network Time Protocol.

NTSC/PAL—National Television System Committee: The first color TV broadcast system was implemented in the United States in 1953. This was based on the NTSC (National Television System Committee) standard. NTSC is used by many countries on the American continent as well as many Asian countries, including Japan. NTSC runs on 525 lines/frame. PAL (Phase Alternating Line) standard was introduced in the early 1960s and implemented in most countries except for France. The PAL standard utilizes a wider channel bandwidth than NTSC, which allows for better picture quality. PAL runs on 625 lines/frame.

NUBC—See the *National Uniform Billing Committee.*

NUBC EDI TAG—The NUBC EDI Technical Advisory Group, which coordinates issues affecting both the NUBC and the X12 standards.

NUCC—See the *National Uniform Claim Committee.*

Nucleus—The core of the atom that is made up of neutrons and protons.

Null—A symbol that means nothing that is included within a message designed to confuse unintended recipients.

Null option—The option to take no action.

Numeric test—An input control method to verify that a field of data contains only numeric digits.

NVA—Network vulnerability assessment.

NVE—Network-visible entity.

NVRAM—Nonvolatile random access memory.

Nyquist Theorem—Theorem that dictates that sampling should occur at a rate that is twice the highest frequency being sampled.

OBJ—(1) Protection Profile evaluation, security objectives. (2) Security Target evaluation, security objectives.

Object—An entity that can have many properties (either declarative, procedural, or both) associated with it.

Object—An instance of a class.

Object identity—In the Object-Oriented paradigm, each object has a unique identifier independent of the values of other properties.

Object program—A program that has been translated from a higher-level source code into machine language.

Object Request Broker (ORB)—A software mechanism by which objects make and receive requests and responses.

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.

Objective information—Quantifiably describes something that is known.

Object-oriented—Any method, language, or system that supports object identity, classification, and encapsulation and specialization. C++, Smalltalk, Objective-C, and Eiffel are examples of object-oriented implementation languages.

Object-Oriented Analysis (OOA)—The specification of requirements in terms of objects with identity that encapsulate properties and operations, messaging, inheritance, polymorphism, and binding.

Object-oriented approach—Combines information and procedures into a single view.

Object-oriented database—Works with traditional database information and also complex data types such as diagrams, schematic drawings, videos, and sound and text documents.

Object-Oriented Database Management System (OODBMS)—A database that stores, retrieves, and updates objects using transaction control, queries, locking, and versioning.

Object-Oriented Design (OOD)—The development activity that specifies the implementation of a system using the conceptual model defined during the analysis phase.

Object-oriented language—A language that supports objects, method resolution, specialization, encapsulation, polymorphism, and inheritance.

Object-oriented programming language—A programming language used to develop object-oriented systems. The language groups together data and instructions into manipulative objects.

Oblivious scheme—See *Blind Scheme*.

Observe, Orient, Decide, Act (OODA)—See *OODA Loop.*

OC—Optical circuit.

OCR—See the Office for Civil Rights.

ODI—Open datalink interface.

Office automation—The application of computer and related technologies to office procedure.

Office for Civil Rights—The HHS entity responsible for enforcing the HIPAA privacy rules.

Office of Management and Budget (OMB)—A federal government agency that has a major role in reviewing proposed federal regulations.

Official Information—That information or material which is owned by, produced for or by, or under the control of the U.S. government.

Off-line authentication certificate—A particular form of authentication information binding an entity to a cryptographic key, certified by a trusted authority, which may be used for authentication without directly interacting with the authority.

Offsite storage—A storage facility located away from the building, housing the primary information processing facility (IPF), and used for storage of computer media such as offline backup data storage files.

Ohm's law—This law applies to any resistive circuit with one of the values unknown and will allow the discovery of the unknown value.

OIG—Office of the Inspector General.

OLE—Microsoft's Object Linking and Embedding technology designed to let applications share functionality through live data exchange and embedded data. Embedded objects are packaged statically within the source application, called the "client;" linked objects launch the "server" applications when instructed by the client application. Linking is the capability to call a program, embedding places data in a foreign program.

OMB—See the *Office of Management and Budget.*

One-time pad—a system that randomly generates a private key, and is used only once to encrypt a message that is then decrypted by the receiver using a matching one-time pad and key. One-time pads have the advantage that there is theoretically no way to "break the code" by analyzing a succession of messages.

Online Analytical Processing (OLAP)—The manipulation of information to support decision-making.

On-line authentication certificate—A particular form of authentication information, certified by a trusted authority, which may be used for authentication following direct interaction with the authority.

Online processing—Often called interactive processing. An operation in which the user works at a terminal or other device that is directly attached or linked to the computer.

Online service—A proprietary, commercial network that provides a variety of information and other services to its subscribers. Commercial online services typically provide their own content, forums (e.g. chat rooms, bulletin boards), e-mail capability, and information available only to subscribers. .

Online system—Applications that allow direct interaction of the user with the computer (CPU) via a CRT, thus enabling the user to receive back an immediate response to data entered (i.e., an airline reservation system). Only one root node can be used at the beginning of the hierarchical structure.

Online training—Runs over the Internet or off a CD-ROM.

Online Transaction Processing (OLTP)—The gathering of input information, processing that information, and updating.

Onward transfer—The transfer of personally identifiable information (PII) by the recipient of the original data to a second recipient. For example, the transfer of PII from an entity in Germany to an entity in the United States constitutes onward transfer of that data. .

OODA Loop—The Observe, Orient, Decide, Act (OODA) cycle (or Boyd Cycle) first introduced by Col. John Boyd, USAF. Refers to steps in the decision-making process. .

Open code—A form of hidden communication which uses an unencrypted message. Jargon code is an example of open code.

Open Network Computing (ONC)—A distributed applications architecture promoted and controlled by a consortium led by Sun Microsystems.

Open network/system—A network or systems in which, at the extremes, unknown parties, possibly in a different state or national jurisdictions will exchange/trade data. To do this, will require an overarching framework which will engender trust and certainty. A user of online services might go through a single authentication process with a trusted third party, receive certification of their public key, and then be able to enter into electronic transactions/data exchanges with merchants, governments, banks etc, using the certificate so provided for multiple purposes.

Open system—A system whose architecture permits components developed by independent organizations or vendors to be combined.

Open Systems Interconnection (OSI)—An international standardization program to facilitate communications among computers from different manufactures. .

OpenMG—A copyright protection technology from Sony that allows recording and playback of digital music data on a personal computer and other supported devices but prevents unauthorized distribution.

Operand—The portion of a computer instruction that references the memory address of an item to be processed.

Operating environment—The total environment in which an information system operates. Includes the physical facility and controls, procedural and administrative controls, personnel controls (e.g., clearance level of the least cleared user).

Operating system—A software program that manages the basic operations of a computer system. It calculates how the computer main memory will be apportioned, how and in what order it will handle tasks assigned to it, how it will manage the flow of information into and out of the main processor, how it will get material to the printer for printing and to the screen for viewing, how it will receive information from the keyboard, etc.

Operating system software—System software that controls the application software and manages how the hardware devices work together.

Operation code—The portion of the computer instruction that identifies the specific processing operation to be performed.

Operational controls—The security controls (i.e., safeguards or countermeasures) for an information system that primarily are implemented and executed by people (as opposed to systems). .

Operational database—A database that supports online transaction processing (OLTP).

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

Operational management—Manages and directs the day-to-day operations and implementations of the goals and strategies.

Operational profile—The set of operations that the software can execute along with the probability with which they will occur.

Operational Security (OPSEC)—Process denying information to potential adversaries about capabilities and intentions by identifying, controlling, and protecting unclassified generic activities.

Operational security information—Transient information related to a single operation or set of operations within the context of an operational association, for example, a user session. Operational security information represents the current security context of the operations and may be passed as parameters to the operational primitives or retrieved from the operations environment as defaults.

Operational status—Either it is (a) operational system is currently in operation, (b) under development system is currently under design, development, or implementation, or (c) undergoing a major modification system is currently undergoing a major conversion or transition. .

Operationally object-oriented—The data model includes generic operators to deal with complex objects in their entirety.

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.

Operator overloading—See *Polymorphism.*

OPSEC—Operations security.

Optical Character Recognition (OCR)—An input method in which handwritten, typewritten, or printed text can be read by photosensitive devices for input to a computer.

Optical disk—A disk that is written to or read from by optical means.

Optical fiber—A form of transmission medium that uses light to encode signals and has the highest transmission rate of any medium.

Optical Mark Recognition (OMR)—Detects the presence of or absence of a mark in a predetermined place (popular for multiple choice exams).

Optical modulation—The process of varying some characteristics of light pulses over a fiber-optic cable in order to pass information from one point to another.

Optical storage—A medium requiring lasers to permanently alter the physical media to create a permanent record. The storage also requires lasers to read stored information from this medium.

Opt-in—An option that gives you complete control over the collection and dissemination of your personal information. A site that provides this option is stating that it will not gather or track information about you unless you knowingly provide such information and consent to the site. .

Opt-out—An option that gives you the choice to prevent personally identifiable information from being used by a particular Web site or shared with third parties. .

Orange Book—Common name used to refer to the DoD Trusted Computing System Evaluation Criteria (TCSEC), DoD 5200.28-STD.

Orange Forces—Forces of the United States operating in an exercise in emulation of the opposing force.

Organizational security policy—Set of laws, rules, and practices that regulates how an organization manages, protects, and distributes sensitive information.

Organized Health Care Arrangement—See Part II, 45 CFR 164.501.

Original classification—An initial determination that information requires protection against unauthorized disclosure in the interest of national security, and a designation of the level of classification.

Original Classifier—An authorized individual in the executive branch who initially determines that particular information requires a specific degree of protection against unauthorized disclosure in the interest of national security and applies the classification designation “Top Secret,” “Secret,” or “Confidential.”.

OSI—Open Systems Interconnection; a seven-layer model from the ISO that defines and standardizes protocols for communicating between systems, networks and devices. .

OSI 7-layer model—The Open System Interconnection 7-layer model is an ISO standard for worldwide communications that defines a framework for implementing protocols in seven layers. Control is passed from one layer to the next, starting at the application layer in one station, and proceeding to the bottom layer, over the channel to the next station and back up the hierarchy.

OSI Reference Model—The seven-layer architecture designed by OSI for open data communications network.

OSPF—Open Shortest Path First.

OUI—Organizationally unique identifier.

Out of band—A LAN term which refers to the capacity to deliver information via modem or other asynchronous connection. Out-of-band signaling refers to signaling that is separated from the channel carrying the information. Signal and control information does not interfere with the data transmission.

Output controls—Techniques and methods for verifying that the results of processing conform to expectations and are communicated only to authorized users.

Output device—A tool used to see, hear, or otherwise accept the results of information-processing requests.

Outsourcing—The delegation of specific work to a third party for a specified length of time, cost, and level of service.

Overlapped processing—The simultaneous execution of input, processing, and output functions by a computer system.

Overlaps—Areas in which too much capability exists. Unnecessary redundancy of coverage in a given area or function.

Overreach interference—Caused by a signal feeding past a repeater (or receive antenna) to the receiving antenna at the next station in the route.

Overseas Security Policy Board (OSPB)—The Overseas Security Policy Board (OSPB) is an interagency group of security professionals from the foreign affairs and intelligence communities who meet regularly to formulate security policy for U.S. missions abroad. The OSPB is chaired by the Director, Diplomatic Security Service.

Overwriting—The obliteration of recorded data by recording different data on the same surface.

P2P—Peer-to-peer infrastructure**.** Often referred to simply as *peer-to-peer*, or abbreviated *P2P*, a type of network in which each workstation has equivalent capabilities and responsibilities. This differs from client/server architectures, in which some computers are dedicated to serving the others. Peer-to-peer networks are generally simpler, but they usually do not offer the same performance under heavy loads.

P3P (Platform for Privacy Preferences Project)—An open privacy specification developed and administered by the World Wide Web Consortium (W3C) that, when implemented, enables people to make informed decisions about how they want to share personal information with Web sites. /.

PABX—Private Automatic Branch Exchange. Telephone switch for use inside a corporation. PABX is the preferred term in Europe, while PBX is used in the United States.

Packet—Logical grouping of information that includes a header containing control information and (usually) user data. Packets are most often used to refer to network layer units of data. The terms “datagram,” “frame,” “message,” and “segment” are also used to describe logical information groupings at various layers of the OSI Reference Model and in various technology circles.

Packet filtering—Controlling access to a network analyzing the attributes of the incoming and outgoing packets and either letting them pass, or denying them based on a list of rules.

Packet Internet Grouper (PING)—A program used to test reachability of destinations by sending them an ICMP echo request and waiting for a reply. The term is used as a verb: “Ping host X to see if it is up.”.

Packet Switch—WAN device that routes packets along the most efficient path and allows a communications channel to be shared by multiple connections. Formerly called an Interface Message Processor (IMP).

Packet Switching—A switching procedure that breaks up messages into fixed-length units (called packets) at the message source. These units may travel along different routes before reaching their intended destination.

PAD—Packet assembler/disassembler.

Padding—A technique used to fill a field, record, or block with default information (e.g., blanks or zeros).

PAG—See Policy Advisory Group.

Page—A basic unit of storage in main memory.

Page fault—A program interruption that occurs when a page that is referred to is not in main memory and must be read from external storage.

Paging—A method of dividing a program into parts called pages and introducing a given page into memory as the processing on the page is required for program execution.

Palm—A type of PDA that runs on the Palm Operating System (Palm OS).

Palm Operating System—The operating system for Palm and Handspring PDAs.

PAP (1)—Password Authentication Protocol.

PAP (2)—Printer Access Protocol (AppleTalk).

PAP (Password Authentication Protocol)—Authentication protocol that allows PPP peers to authenticate one another. The remote router attempting to connect to the local router is required to send an authentication request. Unlike CHAP, PAP passes the password and hostname or username in the clear (unencrypted). PAP does not itself prevent unauthorized access, but merely identifies the remote end. The router or access server then determines if that user is allowed access. PAP is supported only on PPP lines. Compare with *CHAP*.

Parallel connector—Has 25 pins that fit into the corresponding holes in the port. Most printers use parallel connectors.

Parallel conversion—The concurrent use of new system by its users.

Parallel port—The computer's printer port, which in a pinch, allows user access to notebooks and computers that cannot be opened.

Parent—A unit of data in a 1:n relationship with another unit of data called a child, where the parent can exist independently but the child cannot.

Parity—A bit or series of bits appended to a character or block of characters to ensure that the information received is the same as the information that was sent. Parity is used for error detection.

Parity Bit—A bit attached to a byte that is used to check the accuracy of data storage.

Partition—A memory area assigned to a computer program during its execution.

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.

Pascal—A computer programming language designed especially for writing structured programs. This language is based on the use of a minimum set of logical control structures.

Passive response—A response option in intrusion detection in which the system simply reports and records the problem detected, relying on the user to take subsequent action.

Passive system—A system related indirectly to other systems. Passive systems may or may not have a physical connection to other systems, and their logical connection is controlled tightly.

Passive wiretapping—The monitoring or recording of data while it is being transmitted over a communications link.

Password—A word or string of characters that authenticates a user, a specific resource, or an access type.

Password cracker—A password cracker is an application program that is used to identify an unknown or forgotten password to a computer or network resources. It can also be used to help a person obtain unauthorized access to a resource.

Password entropy—Stated in bits, the measure of randomness in a password.

Password sniffing—Eavesdropping on a communications line to capture passwords that are being transmitted unencrypted.

Patchwork—an encoding algorithm that takes random pairs of pixels and brightens the brighter pixel and dulls the duller pixel and encodes one bit of information in the contrast change. This algorithm creates a unique change, and that change indicates the absense or presence of a signature.

Patent—Exclusive right granted to an inventor to produce, sell, and distribute the invention for a specified number of years.

Pattern classification—The step of ASR in which the system matches the user's spoken phonemes to a phoneme sequence stored in an acoustic model database.

Payer—In healthcare, an entity that assumes the risk of paying for medical treatments. This can be an uninsured patient, a self-insured employer, a health plan, or an HMO.

PAYERID— HCFA's term for their pre-HIPAA National Payer ID initiative.

Payload—The amount of information that can be stored in the cover media. Typically the greater the payload the greater the risk of detection.

Payment— See Part II, 45 CFR 164.501.

PBX—Private branch exchange.

PCM—Pulse code modulation.

PCM (Pulse Code Modulation)—A digital scheme for transmitting analog data.

PCS— See *ICD.*

PDA—Personal Digital Assistant. A handheld computer that serves as an organizer for personal information.

PDN—Public data network.

PDU—Protocol data unit.

Peer-entity authentication—The corroboration that a peer entity in an association is the one claimed.

Peer-to-peer network—A network in which a small number of computers share hardware (such as a printer), software, and information.

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

Penetration—A successful unauthorized access to a computer system.

Penetration profile—A delineation of the activities required to effect penetration.

Penetration signature—The description of a situation or set of conditions in which a penetration might occur.

Penetration testing—Security testing in which the evaluators attempt to circumvent the security features of a system based on their understanding of the system design and implementation. The evaluators may be assumed to use all system design and implementation documentation, which may include listings of system source code, manuals, and circuit diagrams. The evaluators work under no constraints other than those applied to ordinary users or implementers of untrusted portions of the component. .

Perceptual masking—a condition where the perception of one element interferes with the perception another.

Perfect forward secrecy—Perfect forward secrecy means that even if a private key is known to an attacker, the attacker cannot decrypt previously sent messages.

Performance—The ability to track service and resource usage levels and to provide feedback on the responsiveness and reliability of the network.

Performance-based—A method for designing learning objectives based on behavioral outcomes, rather than on content that provides benchmarks for evaluating learning effectiveness.

Period—The time it takes a waveform to complete one complete cycle.

Permission marketing —When a person has given a merchant permission to send special offers.

Persistent Object—An object that can survive the process that created it. A persistent object exists until it is explicitly deleted.

Personal agent (or user agent)—An intelligent agent that takes action on the user's behalf.

Personal computer—A commonly used term that refers to a microcomputer. Often called a PC.

Personal Digital Assistant (PDA)—A small hand-held computer that helps surf the Web and perform simple tasks such as note taking, calendaring, appointment scheduling, and maintaining an address book.

Personal finance software—Helps the user maintain a checkbook, prepare a budget, track investments, monitor credit card balances, and pay bills electronically.

Personal Information Management (PIM) software—Helps create and maintain (1) lists, (2) appointments and calendars, and (3) points of contact.

Personal productivity software—Helps the user perform personal tasks — writing a memo, creating a graph, and creating a slide presentation — that can usually be done even if the user does not own a computer.

Personalization—When a Web site can know enough about the user's likes and dislikes that it can fashion offers that are more likely to appeal to the user.

Personally identifiable information—Information that can be traced back to an individual user, e.g. your name, postal address, or e-mail address. Personal user preferences tracked by a Web site via a "cookie" (see definition above) is also considered personally identifiable when linked to other personally identifiable information provided by you online. .

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.

PGP—Pretty Good Privacy. Public key cryptography software based on the RSA cryptographic method.

Phased conversion—The system installation procedure that involves a step-by-step approach for the incremental installation of one portion of a new system at a time.

PHB—Pharmacy Benefits Manager.

PHI—See *Protected Health Information.*

PHP—In Common Criteria, protection of the TSF; TSF physical protection.

PHS—Public Health Service.

Physical layer—The OSI layer that provides the means to activate and use physical connections for bit transmission. In plain terms, the physical layer provides the procedures for transferring a single bit across a physical medium, such as cables.

Physical organization—The packaging of data into fields, records, files, and other structures to make them accessible to a computer system.

Physical security—The measures used to provide physical protection of resources against deliberate and accidental threats.

PictureMarc—A DigiMarc application that embeds an imperceptable digital watermark within an image allowing copyright communication, author recognition and electronic commerce. It is currently bundled with Adobe Photoshop.

PIDAS—Perimeter Intrusion Detection Assessment System.

Piggyback entry—Unauthorized access to a computer system that is gained through another user's legitimate connection.

Ping—Packet Internet groper.

Piracy (or Simple Piracy)—The unauthorized duplication of an original recording for commercial gain without the consent of the rightful owner; or the packaging of pirate copies that is different from the original. Pirate copies are often compilations, such as the "greatest hits" of a specific artist, or a genre collection, such as dance tracks

Pirated software—The unauthorized use, duplication, distribution, or sale of copyrighted software.

Pivot table—Enables to group and summarize information.

Pixel—Short for *picture element,* a pixel is a single point in a graphic image. It is the smallest thing that can be drawn on a computer screen. All computer graphics are made up of a grid of pixels. When these pixels are painted onto the screen, they form an image.

PKI—Public Key Infrastructure.

PL or P. L.—Public Law, as in PL 104-191 (HIPAA).

Plain Old Telephone System (POTS)—What we consider to be the "normal" phone system used with modems. Does not include leased lines or digital lines.

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.).

Plan Administration Functions—See Part II, 45 CFR 164.504.

Plan ID—See National Payer ID.

Plan of action and milestones—A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones. .

Plan Sponsor—An entity that sponsors a health plan. This can be an employer, a union, or some other entity. Also see Part II, 45 CFR 164.501.

Planning phase—Involves determining a solid plan for developing information system.

Platform—Foundation upon which processes and systems are built and which can include hardware, software, firmware, etc.

Platform domain—A security domain encompassing the operating system, the entities and operations it supports and its security policy.

Plotter—A graphics output device in which the computer drives a pen that draws on paper.

PLP—Packet Level Protocol (X.25).

PMD—Physical medium dependent.

PNA adapter card—An expansion card that is put into the user's computer to act as a doorway for information flowing in and out.

Pocket PC—A type of PDA that runs on Pocket PC OS that used to be called Windows CE.

Pocket PC OS (or Windows CE)—The operating system for the Pocket PC PDA.

Pointer—The address of a record (or other data grouping) contained in another record so that a program may access the former record when it has retrieved the latter record. The address can be absolute, relative, or symbolic, and hence the pointer is referred to as absolute, relative, or symbolic.

Pointing stick—Small rubber-like pointing device that causes the pointer to move on the screen as the user applies directional pressure. Popular on notebooks.

Point-of-Presence (POP)—A site where there exists a collection of telecommunications equipment, usually digital leased lines and multi-protocol routers.

Point-of-Sale (POS)—Applications in which purchase transactions are captured in machine-readable form at the point of purchase.

Point-to-Point—A network configuration interconnecting only two points. The connection can be dedicated or switched.

Point-to-Point Protocol (PPP)—The successor to SLIP, PPP provides router-to-router and host-to-network connections over both synchronous and asynchronous circuits.

Polarization—The direction of the electric field, the same as the physical attitude of the antenna (e.g., a vertical antenna transmits a vertically polarized wave). They receive and transmit antennas need to possess the same polarization.

Policy—See *security policy.*

Policy Advisory Group (PAG)— A generic name for many work groups at WEDI and elsewhere.

Polling—A procedure by which a computer controller unit asks terminals and other peripheral devices in a serial fashion if they have any messages to send.

Polymorphism—A request-handling mechanism that selects a method based on the type of target object. This allows the specification of one request that can result in invocation of different methods depending on the type of the target object. Most object-oriented languages support the selection of the appropriate method based on the class of the object (classical polymorphism). A few languages or systems support characteristics of the object, including values and user-defined defaults (generalized polymorphism).

Polymorphism—Having many forms.

POP (1)—Point-of-presence.

POP (2)—Post Office Protocol.

Pop-up ads—An ad that appears in its own window when a user opens or closes a Web page. .

Pop-up blockers—A type of privacy enhancing technology.

Port—(1) An outlet, usually on the exterior of a computer system, that enables peripheral devices to be connected and interfaced with the computer. (2) A numeric value used by the TCP/IP protocol suite that identifies services and applications. For example, HTTP Internet traffic uses port 80.

Portability—The ability to implement and execute software in one type of computing space and have it execute in a different computing space with little or no changes.

Portable Document Format (PDF)—The standard electronic distribution file format for heavily formatted documents such as a presentation resume because it retains the original document formatting.

Ports—An interface point between the CPU and a peripheral device.

POS—Place of service or point of service.

Postpay billing—Billing arrangement between the customer and operator/SvP in which the customer periodically receives a bill for service usage in the past period.

Postscript—A language used to describe the printing of images and text and typically used with laser printing capability. Word processor or desktop publishing applications generate postscript code for higher quality laser products.

POTS—Plain old telephone service.

Power (P)—The measure of the rate at which work can be accomplished.

PP—Protection profile.

PPC—Security Target evaluation, PP claims.

PPO—Preferred Provider Organization.

PPP—Point-to-Point Protocol.

PPS—Prospective Payment System.

PRA—The Paperwork Reduction Act.

Precision Engagement—The ability of joint forces to locate, surveil, discern, and track objectives or targets; select, organize, and use the correct systems; generate desired effects; assess results; and reengage with decisive speed and overwhelming operational tempo as required, throughout the full range of military operations.

Preferred Products List (PPL)—A list of commercially produced equipments that meet TEMPEST and other requirements prescribed by the National Security Agency. This list is included in the NSA Information Systems Security Products and Services Catalogue, issued quarterly and available through the Government Printing Office.

Prepay billing—Billing arrangement between the customer and operator/SvP in which the customer deposits an amount of money in advance, which is subsequently used to pay for service usage.

Preprocessors—Software tools that perform preliminary work on a draft computer program before it is completely tested on the computer.

Presentation layer—The layer of the ISO Reference Model responsible for formatting and converting data to meet the requirements of the particular system being utilized.

Presentation resume—A format-sensitive document created in a word processor to outline job qualifications in one to two printed pages.

Presentation software—Helps create and edit information that will appear in electronic slides.

Pretty Good Privacy (PGP)—PGP provides confidentiality and authentication services for electronic mail and file storage applications. Developed by Phil Zimmerman and distributed for free on the Internet. Widely used by the Internet technical community.

PRG—Procedure-Related Group.

PRI—Primary Rate Interface (ISDN).

Pricer or Repricer—A person, an organization, or a software package that reviews procedures, diagnoses, fee schedules, and other data and determines the eligible amount for a given healthcare service or supply. Additional criteria can then be applied to determine the actual allowance, or payment, amount.

Primary Key—An attribute that contains values that uniquely identifies the record in which the key exists.

Primary Mission Area—Synonymous with Primary Warfare Mission Area (PWMA). A warfare mission area concerned with a specific, major phase or portion of naval warfare.

Primary Rate Interface (PRI)—Provides the same throughput as a T-1, 1.544 Mbps, has 23 B or bearer channels, which run at 64 kbps, and a D or data channel, which runs at 16 kbps.

Primary service—An independent category of service such as operating system services, communication services and data management services. Each primary service provides a discrete set of functionality. Each primary service inherently includes generic qualities such as usability, manageability and security. Security services are therefore not primary services but are invoked as part of the provision of primary services by the primary service provider.

Principal—An entity whose identity can be authenticated.

Principle of Least Privilege—A security procedure under which users are granted only the minimum access authorization they need to perform required tasks.

Print suppress—The elimination of the printing of characters to preserve their secrecy — for example, the characters of a password as they are keyed by a user at a terminal or station on the network.

Privacy—1. The prevention of unauthorized access and manipulation of data. 2. The right of individuals to control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

Privacy Act of 1974—The federal law that allows individuals to know what information about them is on file and how it is used by all government agencies and their contractors. The 1986 Electronic Communication Act is an extension of the Privacy Act.

Privacy Enhanced Mail (PEM)—Internet email standard that provides confidentiality, authentication, and message integrity using various encryption methods. Not widely deployed in the Internet.

Privacy Impact Assessment (PIA)—An analysis of how information is handled (1) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (2) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (3) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

Privacy Invasive Technologies (PITs)—Describes the many technologies that intrude into privacy. Among the host of examples are data-trail generation through the denial of anonymity, data-trail intensification (e.g., identified phones, stored-value cards, and intelligent transportation systems), data warehousing and data mining, stored biometrics, and imposed biometrics. .

Privacy policy—An organization's requirements for complying with privacy regulations and directives. .

Privacy policy in standardized machine-readable format—A statement about site privacy practices written in a standard computer language (not English text) that can be read automatically by a Web browser. .

Privacy Protection—The establishment of appropriate administrative, technical, and physical safeguards to protect the security and confidentiality of data records against anticipated threats or hazards

Privacy Protection—The establishment of appropriate administrative, technical, and physical safeguards to protect the security and confidentiality of data records against anticipated threats or hazards that could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual about whom such information is maintained.

Privacy seal—An online seal awarded by one of multiple privacy certification vendors to Web sites that agree to post their privacy practices openly via privacy statements, as well as adhere to enforcement procedures that ensure that their privacy promises are met. When you click on the privacy seal, typically you're taken directly to the privacy statement of the certified Web site.

Privacy statement—A page or pages on a Web site that lay out its privacy policies, i.e. what personal information is collected by the site, how it will be used, whom it will be shared with, and whether you have the option to exercise control over how your information will be used. .

Private Branch Exchange (PBX)—A small version of the phone company's central switching office. Also known as a private automatic branch exchange.

Private Branch Exchange (PBX)—A central telecommunications switching station that an organization uses for its own purposes.

Private Key—The private or secret key of a key pair, which must be kept confidential and is used to decrypt messages encrypted with the public key, or to digitally sign messages which can then be validated with the public key.

Private Network—A network established and operated by a private organization for the benefit of members of the organization.

Privilege—A right granted to an individual, a program, or a process.

Privileged instructions—A set of instructions generally executable only when the computer system is operating in the executive state (e.g., while handling interrupts). These special instructions are typically designed to control such protection features as the storage protection features.

PRO—Professional Review Organization or Peer Review Organization.

Problem—Any deviation from predefined standards.

Problem reporting—The method of identifying, tracking, and assigning attributes to problems detected within the software product, deliverables, or within the development processes.

Procedural language—A computer programming language in which the programmer must determine the logical sequence of program execution as well as the processing required.

Procedure—Required "how-to" instructions that support some part of a policy or standard, which state "what to do.".

Procedure division—A section of a COBOL program that contains statements that direct computer processing operations.

Procedure view—Contains all of the procedures within a system.

Process—A sequence of activities.

Process description—A narrative that describes in sequence the processing activities that take place in a computer system and the procedures for completing each activity.

Processing controls—Techniques and methods used to ensure that processing produces correct results.

Processor—The hardware unit containing the functions of memory and the central processing unit.

Product Certification Center—A facility that certifies the technical security integrity of communications equipment. The equipment is handled and used within secure channels.

Professional Courier (or Diplomatic Courier)—A person specifically employed and provided with official documentation by the U.S. Department of State to transport properly prepared, addressed, and documented diplomatic pouches between the Department and its Foreign Service posts and across other international boundaries.

Profile filtering—Requires that the user choose terms or enter keywords to provide a more personal picture of preferences.

Profiling—Analyzing a program to determine how much time is spent in different parts of the program during execution. .

Program analyzers—Software tools that modify or monitor the operation of an application program to allow information about its operating characteristics to be collected automatically.

Program development process—The activities involved in developing computer programs, including problem analysis, program design, process design, program coding, debugging, and testing.

Program maintenance—The process of altering program code or instructions to meet new or changing requirements.

Program Manager—The person ultimately responsible for the overall procurement, development, integration, modification, or operation and maintenance of the IS.

Programmable Read-Only Memory (PROM)—Computer memory chips that can be programmed permanently to carry out a defined process.

Programmer—The individual who designs and develops computer programs.

Programmer/Analyst—The individual who analyzes processing requirements and then designs and develops computer programs to direct processing.

Programming language—A language with special syntax and style conventions for coding computer programs.

Programming Language/1 (PL/1)—A general-purpose, high-level language that combines business and scientific processing features. The language contains advanced features for experienced programmers yet can be easily learned by novice programmers.

Programming specifications—The complete description of input, processing, output, and storage requirements necessary to code a computer program.

Project manager—An individual who is an expert in project planning and management, defines and develops the project plan, and tracks the plan to ensure all key project milestones are completed on time.

Project milestone—Key date by which a certain group of activities needs to be performed.

Project plan—Defines the what, when, and who questions of system development including all activities to be performed, the individuals or resources who will perform the activities, and the time required to complete each activity.

Project scope—Clearly defines the high-level system requirements.

Project scope document—A written definition of the project scope and usually no longer than a paragraph.

Project team—A team designed to accomplish specific one-time goals, which is disbanded once the project is complete.

Prolog—A language widely used in the field of artificial intelligence.

PROM—Programmable read-only memory.

Proof of correctness—The use of mathematical logic to infer that a relation between program variables assumed true at the program entry implies that another relation between program variables holds at program exit.

Proof-of-concept prototype—A prototype used to prove the technical feasibility of a proposed system.

Protect—To keep information systems away from intentional, unintentional, and natural threats: (1) preclude an adversary from gaining access to information for the purpose of destroying, corrupting, or manipulating such information; or (2) deny use of information systems to access, manipulate, and transmit mission-essential information.

Protected Distribution System (PDS)—Wire line or fiber optic distribution system used to transmit unencrypted classified national security information through an area of lesser classification or control.

Protected Health Information (PHI)—See Part II, 45 CFR 164.501.

Protection ring—A hierarchy of access modes through which a computer system enforces the access rights granted to each user, program, and process, ensuring that each operates only within its authorized access mode.

Protection schema—An outline detailing the type of access users may have to a database or application system, given a user's need-to-know; e.g., read, write, modify, delete, create, execute, and append.

Protective layers—Mechanisms for insuring the integrity of systems or data. See *Defense in Depth.*

Protocol—A set of instructions required to initiate and maintain communication between sender and receiver devices.

Protocol Analyzer—A data communications testing unit set that enables a network engineer to observe bit patterns and simulate network elements.

Protocol Data Unit (PDU)—This is OSI terminology for "packet." A PDU is a data object exchanged by protocol machines (entities) within a given layer. PDUs consist of both protocol control information (PCI) and user data.

Protons—A heavy subatomic particle that carries a positive charge.

Prototype—A usable system or subcomponent that is built inexpensively or quickly with the intention of modifying or replacing it.

Provider Taxonomy Codes—An administrative code set for identifying the provider type and area of specialization for all healthcare providers. A given provider can have several Provider Taxonomy Codes. This code set is used in the X12 278 Referral Certification and Authorization and the X12 837 Claim transactions, and is maintained by the NUCC.

Proxy server—Proxy server is a server that acts as an intermediary between a remote user and the servers that run the desired applications. Typical proxies accept a connection from a user, make a decision as to whether or not client IP address is permitted to use the proxy, perhaps perform additional authentication, and complete a connection to a remote destination on behalf of the user.

PRS—Resource utilization, priority of service.

PSDN—Packet-Switched Data Network.

PSE—Privacy, pseudonymity.

Pseudocode—Program processing specifications that can be prepared as structured English-like statements which can then be easily converted into source code.

Pseudoflow—An apparent loophole deliberately implanted in an operating system program as a trap for intruders.

Pseudonymity—A condition in which you have taken on an assumed identity. .

PSK—Phase shift keying.

PSN—Packet-switched network.

PSNP—Partial Sequence Number PDU.

PSPDN—Packet-switched public data network.

PSTN—Public switched telephone network.

Psychographic filtering—Anticipates the user's preferences based on the answers given to a questionnaire.

Psychotherapy notes—See Part II, 45 CFR 164.501.

PTT—Post, telephone, and telegraph.

Public Health Authority—See Part II, 45 CFR 164.501.

Public key—In an asymmetric cryptography scheme, the key that may be widely published to enable the operation of the scheme. Typically, a public key can be used to encrypt, but not decrypt or to validate a signature, but not to sign.

Public key cryptography—An asymmetric cryptosystem where the encrypting and decrypting keys are different and it is computationally infeasible to calculate one form the other, given the encrypting algorithm. In public key cryptography, the encrypting key is made public , but the decrypting key is kept secret.

Public Key Cryptography Standards—Public Key Cryptography Standards (PKCS) are specifications produced by RSA Laboratories in cooperation with secure systems developers worldwide for the purpose of accelerating the deployment of Public-Key Cryptography.

Public key cryptosystem—An asymmetric cryptosystem that uses a public key and a corresponding private key.362.

Public key encryption—An encryption scheme where two pairs of algorithmic keys (one private and one public) are used to encrypt and decrypt messages, files, etc.

Public key infrastructure—Supporting infrastructure, including non-technical aspects, for the management of public keys.

Public network—A network on which the organization competes for time with others.

Public Switched Telephone Network (PSTN)—Refers to the local, long distance, and international phone system which we use every day. In some countries, it is a single phone company. In countries with competition, PSTN refers to the entire interconnected collections of local, long distance, and international phone companies, of which there could be thousands.

Pulse Amplitude Modulation (PAM)—The first step in converting analog waveforms into digital signals for transmission.

Pulse Code Modulation (PCM)—The most common and most important method that a telephone system in North America can use to sample a voice signal and convert that sample into an equivalent digital code. PCM is a digital modulation method that encodes a pulse amplitude modulated signal into a PCM signal.

Purging—The orderly review of storage and removal of inactive or obsolete data files.

Push technology—An environment in which businesses and organizations come to the user with information, services, and product offerings based on the user profile.

PVC—Permanent virtual circuit.

QA—Quality assurance.

QAM—Quadrature Amplitude Modulation.

QC—Quality control.

QoS—Quality of service.

Qualitative—Inductive analytical approaches that are oriented toward relative, non-measurable, and subjective values, such as expert judgment.

Quality—The totality of features and characteristics of a product or service that bear on its ability to meet stated or implied needs.

Quality Assurance—An overview process that entails planning and systematic actions to ensure that a project is following good quality management practices.

Quality Control—Process by which product quality is compared with standards.

Quality of Service (QoS)—The service level defined by a service agreement between a network user and a network provider, which guarantees a certain level of bandwidth and data flow rates.

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

Quantitizing—The systematic method of providing standard binary numbering to PAM samples for PCM conversion.

Query and reporting tools—Similar to QBE tools, SQL, and report generators in the typical database environment.

Query language—A language that enables a user to interact indirectly with a DBMS to retrieve and possibly modify data held under the DBMS.

Query-by-Example tools (QBE)—Helps the user graphically design the answer to a question.

Queue—A waiting line in which a set of computer programs is in secondary storage awaiting processing.

Radiation field—The radio frequency field that is created around the antenna and has specific properties that affect the signal transmission.

RADIUS—Remote Authentication Dial-In User Service.

RADIUS (Remote Dial-In User Service)—Database for authenticating modem and ISDN connections and for tracking connection time. Remote authentication dial-in user service. A protocol used to authenticate remote users and wireless connections.

RAID (Redundant Arrays of Inexpensive Disks)—Instead of using one large disk to store data, you use many smaller disks (because they are cheaper). *See* disk mirroring and duplexing. An approach to using many low-cost drives as a group to improve performance, yet also provides a degree of redundancy that makes the chance of data loss remote.

Rain attenuation or raindrop absorption—The scattering of the microwave signal, which can cause signal loss in transmissions.

Rainbow series—A multi-volume set of publications on Information Assurance, Information Security and related topics. Published by the National Computer Security Center (NCSC) at the National Security Agency (NSA) in Fort Meade, MD. Each volume is published under a different color cover, hence the term "Rainbow" series.

Rainbow tables—A set of tools and techniques used for cracking MS Windows passwords.

RAM—A type of computer memory that can be accessed randomly; that is, any byte of memory can be accessed without touching the preceding bytes. RAM is the most common type of memory found in computers and other devices, such as printers. There are two basic types of RAM: dynamic RAM (DRAM) and static RAM (SRAM).

Random access—A method that allows records to be read from and written to disk media without regard to the order of their record key.

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

Range—The distance a signal travels before it degrades and needs to be repeated.

RARP (Reverse Address Resolution Protocol)—Protocol in the TCP/IP stack that provides a method for finding IP addresses based on MAC addresses. Compare with *Address Resolution Protocol (ARP).*

Raster image—An image that is composed of small points of color data called pixels. Raster images allow the representation complex shapes and colors in a relatively small file format. Photographs are represented using raster images.

RBOCs—Regional Bell operating companies.

RCP—Remote Copy Protocol.

RCR—Development, representation correspondence.

RCV—Protection of the TSF, trusted recovery.

Reaccreditation—The official management decision to continue operating a previously accredited system. .

Reach—An aggregate measure of the degree to which information is shared.

React—To respond to threat activity within information systems, when detected, and mitigate the consequences by taking appropriate action to incidents that threaten information and information systems.

Read-Only Memory (ROM)—Computer memory chips with preprogrammed circuits for storing such software as word processors and spreadsheets.

Reality—The real world.

Real-time processing—Computer processing that generates output fast enough to support multiple activities being performed concurrently.

Real-time reaction—A response to a penetration attempt that can prevent actual penetration because the attempt is detected and diagnosed in time.

Reassembly—The process by which an IP datagram is "put back together" at the receiving hosts after having been fragmented in transit.

Recertification—A reassessment of the technical and non-technical security features and other safeguards of a system made in support of the reaccreditation process. .

Reciprocal agreement—Emergency processing agreements between two or more organizations with similar equipment or applications. Typically, participants promise to provide processing time to each other when an emergency arises.

Reciprocity—An antenna characteristic that essentially states that the antenna is the same regardless of whether it is sending or receiving electromagnetic energy.

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

Record block—A group or collection of records appearing between interblock gaps on magnetic storage media. This group of records is handled as a single entity in computer processing.

Record blocking—A technique of writing several records to magnetic storage media in between interblock gaps or spaces.

Record material—All books, papers, maps, photographs, or other documentary materials, regardless of physical form or characteristics, made or received by the U.S. government in connection with the transaction of public business and preserved or appropriated by an agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, or other activities of any agency of the government, or because of the informational data contained therein.

Recording Industry Association of America (RIAA)—A trade group that represents the U.S. recording industry. The RIAA works to create a business and legal environment that supports the record industry and seeks to protect intellectual property rights.

Recovery—The restoration of the information processing facility or other related assets following physical destruction or damage.

Recovery Point Objective (RPO)—A measurement of the point prior to an outage to which data are to be restored.

Recovery Procedures—The action necessary to restore a system's computational capability and data files after system failure or penetration.

Recovery Time Objective (RTO)—The amount of time allowed for the recovery of a business function or resource after a disaster occurs.

Rectifier—A diode designed to be placed in an alternating current circuit, used for converting AC to DC.

Recurring decision—A decision that you have to make repeatedly and often periodically, whether weekly, monthly, quarterly, or yearly.

Recursion—The definition of something in terms of itself. For example, a bill of material is usually defined in terms of itself.

Red—Designation applied to information systems, and associated areas, circuits, components, and equipment in which national security information is being processed.

Red Book—Common name used to refer to the Network Interpretation of the TCSEC (Orange Book). Originally referred to in some circles as the "White Book.".

Red Forces—Forces of countries considered unfriendly to the United States and her Allies.

Red Team—A group of people duly authorized to conduct attacks against friendly information systems, under prescribed conditions, for the purpose of revealing the capabilities and limitations of the information assurance posture of a system under test. For purposes of operational testing, the Red team will operate in as operationally realistic an environment as feasible and will conduct its operations in accordance with the approved operational test plan.

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 nonnational security information (BLACK) in the same form.

Red-Black separation—The requirement for physical spacing between "red" and "black" processing systems and their components, including signal and power lines.

Reduced Instruction Set Computing (RISC)—A method of processing by which the set of instructions available to the computer is a subset of that found on conventional computers.

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.

Redundant control capability—Use of active or passive replacement, for example, throughout the network components (i.e., network nodes, connectivity, and control stations) to enhance reliability, reduce threat of single-point-of-failure, enhance survivability, and provide excess capacity.

Redundant site—A recovery strategy involving the duplication of key information technology components, including data, or other key business processes, whereby fast recovery can take place. The redundant site usually is located away from the original.

Reference configuration—A combination of functional groups and reference points that shows possible network arrangements.

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

Referential attributes—The facts that tie an instance of one object to an instance of another object.

Referential integrity—The assurance that an object handle identifies a single object. The facility of a DBMS that ensures the validity of predefined relationships.

Referrer Field—The referrer header field (mistakenly spelled referer in the HTTP standard) is a unit of information that contains the URL of the site you are currently in. The referrer header field is sent automatically to any site you are about to visit when clicking a link. Referrer headers allow reading patterns to be studied and reverse links drawn. The address of the page might contain privacy information (such as your name or e-mail address), or might reveal personal interests that you would rather keep private.

Reflections—When the microwave signal traverses a body of water or fog bank and causes multipath conditions.

Regenstrief Institute—A research foundation for improving healthcare by optimizing the capture, analysis, content, and delivery of healthcare information. Regenstrief maintains the LOINC coding system that is being considered for use as part of the HIPAA claim attachments standard.

Regional Diplomatic Courier Officer (RDCO)—The RDCO oversees the operations of a regional diplomatic courier division.

Regression testing—The rerunning of test cases that a program has previously executed correctly to detect errors created during software correction or modification. Tests used to verify a previously tested system whenever it is modified.

Relation—Describes each two-dimensional table or file in the relation model (hence its name relational database model).

Relational database—In a relational database, data is organized in two-dimensional tables or relations.

Relevance—Related to the matter at hand; directly bearing upon the current matter.

Reliability—The probability that a system or service will perform in a satisfactory manner for a given period of time when used under specific operating conditions.

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.

Relying third party—The entity, such as a merchant, offering goods or services online that will receive a certificate as part of a process of completing transactions with the user.

Remanence—The residual magnetism that remains on magnetic storage media after degaussing.

Remediation plan—See *plan of action and milestones.*

Remote access—The ability to dial into a computer over a local telephone number using a number of digital access techniques.

Remote Authentication Dial-In User Service (RADIUS)—A security and authentication mechanism for remote access.

Remote diagnostic facility—An off-premise diagnostic, maintenance, and programming facility authorized to perform functions on the Department computerized telephone system via an external network trunk connection.

Remote File System (RFS)—A distributed file system, similar to NFS, developed by AT&T and distributed with their UNIX System V operating system. See Network File System.

Remote Procedure Call (RPC)—An easy and popular paradigm for implementing the client/server model of distributed computing. A request is sent to a remote system to execute a designated procedure, using arguments supplied, and the result returned to the caller.

Repeater—A device that propagates electrical signals from one cable to another without making routing decisions or providing packet filtering. In OSI terminology, a repeater is a physical layer intermediate system. See bridge and router.

Replay—A type of security threat that occurs when an exchange is captured and resent at a later time to confuse the original recipients.

Replication—The process of keeping a copy of data through either shadowing or caching.

Report—Printed or displayed output that communicates the content of files and other activities. The output is typically organized and easily read.

Report Program Generator (RPG)—A nonprocedural programming language used for many business applications.

Report writing—The process of accessing data from files and generating it as information in the form of output.

Repudiation—Denying that you did something, or sent some message.

REQ—(1) Protection Profile evaluation, IT security requirements. (2) Security Target evaluation, IT security requirements.

Request for Comments (RFC)—The document series, begun in 1969, that describes the Internet suite of protocols and related experiments. Not all (in fact, very few) RFCs describe Internet standards, but all Internet standards are written up as RFCs.

Request for Proposal (RFP)—A formal document that describes in detail logical requirements for a proposed system and invites outsourcing organizations (vendors) to submit bids for its development.

Required by Law—See Part II, 45 CFR 164.501.

Requirement definition document—Defines all of the business requirements, prioritizes them in order of business importance, and places them in a formal comprehensive document.

Residual risks—The risk associated with an event when the control is in place to reduce the effect or likelihood of that event being taken into account.

Residue—Data left in storage after processing operations and before degaussing or rewriting has occurred.

Resistance —(1) The opposition to the flow of electric charge and is generally the function of the number of free electrons available to conduct the electric current. (2) Capability of a system to repel attacks.

Resistor—A component made of a material that has a specified resistance or opposition to the flow of electrical current. A resistor is designed to oppose but not completely obstruct the passage of electrical current.

Resolution of a printer—The number of dots per inch (dpi) a printer produces, which is the same principle as the resolution in a monitor.

Resolution of a screen—The number of pixels a screen has. Pixels (picture elements) are the dots that make up an image on the screen.

Resonant frequency—The frequency where inductive reactance equals capacitive reactance. Helps to define the maximum current or maximum voltage in a circuit.

Resource—In a computer system, any function, device, or data collection that can be allocated to users or programs.

Resource sharing—In a computer system, the concurrent use of a resource by more than one user, job, or program.

Restricted area—A specifically designated and posted area in which classified information or material is located or in which sensitive functions are performed, access to which is controlled and to which only authorized personnel are admitted.

Result of interception—Information relating to a target service, including the CC and IRI, which is passed by an NWO/AP/SvP to an LEA. IRI shall be provided whether or not call activity is taking place.

REV—Security management, revocation.

RF Shielding—The application of materials to surfaces of a building, room, or a room within a room, that makes the surface largely impervious to electromagnetic energy. As a technical security countermeasure, it is used to contain or dissipate emanations from information processing equipment, and to prevent interference by externally generated energy.

RFA—The Regulatory Flexibility Act.

RFC—Request for Comments.

RFI—Radio frequency interference.

RFID (radio frequency identification system)—An automatic identification and data capture system comprising one or more readers and one or more tags in which data transfer is achieved by means of suitable modulated inductive or radiating electromagnetic carriers. .

RGB (Red, Green, Blue)—Refers to a system for representing the colors to be used on a computer display.

Richness—Defined by three aspects of the information itself: bandwidth (the amount of information), the degree to which the information is customized, and interactivity (the extent of two way communication).

Ring side—The side of the cable pair that when measured will read –48 V DC.

RIP (Routing Information Protocol)—User data protection residual information protection.

RISC—Reduced Instruction Set Computer.

Risk—The probability that a particular security threat will exploit a particular vulnerability.

Risk analysis—An analysis that examines an organization’s information resources, its existing controls, and its remaining organization and computer system vulnerabilities. It combines the loss potential for each resource or combination of resources with an estimated rate of occurrence to establish a potential level of damage in dollars or other assets.

Risk assessment—A process used to identify and evaluate risks and their potential effects.

Risk avoidance—The process for systematically avoiding risk. Security awareness can lead to a better education staff, which can lead to certain risks being avoided.

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 index—The disparity between the minimum clearance or authorization of system users and the maximum sensitivity (e.g., classification and categories) of data processed by a system.

Risk management—The discipline of identifying and measuring security risks associated with an information system, and controlling and reducing those risks to an acceptable level. The goal of risk management is to invest organizational resources to mitigate security risks in a cost-effective manner, while enabling timely and effective mission accomplishment. Risk management is an important aspect of information assurance and defense-in-depth.

Risk mitigation—While some risks cannot be avoided, they can be minimized or mitigated by putting controls into place to mitigate the risk once an incident occurs.

Risk transfer—The process of transferring risk. An example can include transferring the risk of a building fire to an insurance company.

RJE—Remote job entry.

rlogin—A service offered by Berkeley UNIX that allows users of one machine to log into other UNIX systems (for which they are authorized) and interact as if their terminals were connected directly. Similar to Telnet.

RLP—Remote Location Protocol.

RMON—Remote monitoring.

Robot—A mechanical device equipped with simulated human senses and the capability of taking action on its own.

Robotics—The use of automated equipment for production work and other mechanical tasks.

Robust watermark—a watermark, which is very resistant to destruction under any image manipulation. This is useful in verifying ownership of an image suspected of misappropriation. Digital detection of the watermark would indicate the source of the image.

Robustness—The system's ability to operate despite service interruption, system errors and other anomalous events.

ROI—Return on investment.

ROL—User data protection rollback.

Role—A job type defined in terms of a set of responsibilities.

Role-based—When mapped to job function, assumes that a person will take on different roles, over time, within an organization and different responsibilities in relation to IT systems.

Roles and responsibilities—Functions performed by someone in a specific situation and obligations to tasks or duties for which that person is accountable.

Rollback—(1) Restoration of a system to its former condition after it has switched to a fallback mode of operation when the cause of the fallback has been removed. (2) The restoration of the database to an original position or condition often after major damage to the physical medium. (3) The restoration of the information processing facility or other related assets following physical destruction or damage.

ROM—See *read-only memory.*

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.

Rootkits—(1) User-level rootkits: Programs that "infect" program files that are executed by the user and run under the user account's privileges (for example, the Explorer.exe or Word.exe program) (2) Kernel-level rootkits: Programs that "infect" functions belonging to the operating system kernel (i.e., the core Windows operating system) and are used by hundreds of applications (including the Windows API). Kernel-mode rootkits will modify (i.e., hijack) internal operating system functions that return lists of files, processes, and open ports .

Rotary (or pulse) dialing—The circular telephone dial. As it returns to its normal position, it opens and closes the electrical loop sent by the central office. Rotary dial telephones momentarily break the DC circuit to represent the digits dialed.

Router—(1) A system responsible for making decisions about which of several paths network (or Internet) traffic will follow. To do this, it uses a routing protocol to gain information about the network, and algorithms to choose the best route based on several criteria known as "routing metrics." (2) A network node connected to two or more networks. It is used to send data from one network (such as 137.13.45.0) to a second network (such as 43.24.56.0). The networks could both use Ethernet, or one could be Ethernet and the other could be ATM (or some other networking technology). As long as both speak common protocols (such as the TCP/IP protocol suite), they can communicate.

RPC—Remote procedure call.

RPL—Protection of the TSF; replay detection.

RSA—A public key cryptosystem developed by Rivest, Shamir and Adleman. The RSA has two different keys, the public encryption key and the secret decryption key. The strength of the RSA depends on the difficulty of the prime number factorization. For applications with high-level security, the number of the decryption key bits should be greater than 512 bits. RSA is used for both encryption and digital signatures.

RSA—Resource utilization, resource allocation.

RTFM—Read the "fine" manual.

RTMP—Routing Table Maintenance Protocol (AppleTalk).

RTP—Real-Time Transport Protocol.

Rule based expert—The type of expert system that expresses the problem-solving process as rules.

Rule-Based Security Policy—A security policy based on global rules imposed for all subjects. These rules usually rely on a comparison of the sensitivity of the objects being accessed and the possession of corresponding attributes by the subjects requesting access.

Rules—Constraints.

Rules of behavior—The rules that have been established and implemented concerning use of, security in, and acceptable level of risk for the system. Rules will clearly delineate responsibilities and expected behavior of all individuals with access to the system. Rules should cover such matters as working at home, dial-in access, connection to the Internet, use of copyrighted works, unofficial use of federal government equipment, the assignment and limitation of system privileges, and individual accountability. .

RVM—Protection of the TSF, reference mediation.

RVS—Relative Value Scale.

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

SA (1)—Source address.

SA (2)—Security Association.

SAA—Security audit analysis.

SABM—Set asynchronous balanced mode.

SABME—Set asynchronous balanced mode extended.

SAE—Security management, security attribute expiration.

Safe Harbor Principles—The set of rules to which U.S. businesses that want to trade with the European Union (EU) must adhere.

Safeguards—Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Synonymous with security controls and countermeasures.

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. (2) The probability of a safety-related system satisfactorily performing the required safety functions under all stated conditions within a stated period of time. .

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. .

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. .

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.

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. .

Sales Force Automation (SFA) System—Automatically tracks all of the steps in the sales process.

Salt—Salt is a string of random (or pseudo-random) bits concatenated with a key or password to reduce the probability of pre-computation attacks.

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.

Sanitize—The degaussing or overwriting of information on magnetic or other storage media.

Sanitizing—The degaussing or overwriting of sensitive information in magnetic or other storage media.

SAP (1)—Service access point.

SAP(2)—Service Advertisement Protocol (Novell).

SAR—Security audit review.

Sarbanes–Oxley Act of 2002—The most dramatic change to federal securities laws since the 1930s, the Act radically redesigns federal regulation of public company corporate governance and reporting obligations. It also significantly tightens accountability standards for directors and officers, auditors, securities analysts, and legal counsel.

SAS—Single attached station.

Satellite modem—A modem that allows Internet access from a satellite dish.

SC— Subcommittee.

Scalability—The likelihood that an artifact can be extended to provide additional functionality with little or no additional effort.

Scalability—Refers to how well a system can adapt to increased demands.

Scannable resume (ASCII resume, plain-text resume)—Designed to be evaluated by skills-extraction software and typically contains all resume content without any formatting.

Scanner—Captures images, photos, and artwork that already exist on paper.

Scavenging—The searching of residue for the purpose of unauthorized data acquisition.

Scheduling program—A systems program that schedules and monitors the processing of production jobs in the computer system.

SCHIP— The State Children’s Health Insurance Program.

SCL—Security certification level (see certification level).

Scope creep—Occurs when the scope of the project increases.

SCP—CM scope.

Script bunny (or script kiddie)—Someone who would like to be a hacker but does not have much technical expertise.

Scripts—Executable programs used to perform specified tasks for servers and clients.

SDH—Synchronous digital hierarchy.

SDI—User data protection, stored data integrity.

SDLC—System development life cycle.

SDO—Under HIPAA, Standards Development Organization.

SDU—Service data unit.

Search Engine—A program written to allow users to search the Web for documents that match user-specified parameters.

Secrecy—A security principle that keeps information from being disclosed to anyone not authorized to access it.

Secret key cryptography—A cryptographic system where encryption and decryption are performed using the same key.

Secretary—Under HIPAA, this refers to the secretary of HHS or his designated representatives. Also see Part II, 45 CFR 160.103.

Secure Digital Music Initiative (SDMI)—Forum of more than 160 companies and organizations representing a broad spectrum of information technology and consumer electronics businesses, Internet service providers, security technology companies, and members of the worldwide recording industry working to develop voluntary, open standards for digital music. SDMI is helping to enable the widespread Internet distribution of music by adopting a framework that artists and recording and technology companies can use to develop new business models.

helping to enable the widespread Internet distribution of music by adopting a framework that artists and recording and technology companies can use to develop new business models.

Secure Electronic Transaction (SET)—The SET specification has been developed to allow for secure credit card and offline debit card (check card) transactions over the World Wide Web.

Secure interoperability—The ability to have secure, successful transactions. Today’s interoperability expands that previous focus to also include information assurance considerations, and include the requirement to formally assess whether that traditional, successful transaction is also secure (i.e., secure interoperability meaning a secure, successful transaction exists).

Secure operating system—An operating system that effectively controls hardware, software, and firmware functions to provide the level of protection appropriate to the value of the data resources managed by this operating system.

Secure room—Any room with floor-to-ceiling, slab-to-slab construction of some substantial material, i.e., concrete, brick, cinder block, plywood, or plaster board. Any window areas or penetrations of wall areas over 15.25 cm (six inches) must be covered with either grilling or substantial type material. Entrance doors must be constructed of solid wood, metal, etc., and be capable of holding a DS-approved three-way combination lock with interior extension.

Secure Socket Layer (SSL)—A protocol developed by Netscape for transmitting private documents via the Internet. SSL works by using a public key to encrypt data that is transferred over the SSL connection.

Secure voice—Systems in which transmitted conversations are encrypted to make them unintelligible to anyone except the intended recipient. Within the context of Department security standards, secure voice systems must also have protective features included in the environment of the systems terminals.

Security—(1) Freedom from undesirable events, such as malicious and accidental misuse; how well a system resists penetrations by outsiders and misuse by insiders. (2) The protection of system resources from accidental or malicious access, use, modification, destruction, or disclosure. (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. Security concerns transcend the boundaries of an automated system.

Security accreditation—See *accreditation.*

Security anomaly—An irregularity possibly indicative of a security breach, an attempt to breach security, or of noncompliance with security standards, policy, or procedures.

Security association—A security association is a set of parameters which defines all the security services and mechanisms used for protecting the communication. A security association is bound to a specific security protocol.

Security audit—An examination of data security procedures and measures to evaluate their adequacy and compliance with established policy.

Security authorization—See *accreditation.*

Security category—The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, or individuals. .

Security classification designations—Refers to “Top Secret,” and “Secret,” and “Confidential” designations on classified information or material.

Security controls—Techniques and methods to ensure that only authorized users can access the computer information system and its resources.

Security domain—A set of subjects, their information objects, and a common security policy.

Security equipment—Protective devices such as intrusion alarms, safes, locks, and destruction equipment which provide physical or technical surveillance protection as their primary purpose.

Security evaluation—An evaluation done to assess the degree of trust that can be placed in systems for the secure handling of sensitive information. One type, a product evaluation, is an evaluation performed on the hardware and software features and assurances of a computer product from a perspective that excludes the application environment. The other type, a system evaluation, is done for the purpose of assessing a system's security safeguards with respect to a specific operational mission and is a major step in the certification and accreditation process.

Security filter—A set of software or firmware routines and techniques employed in a computer system to prevent automatic forwarding of specified data over unprotected links or to unauthorized persons.

Security goals—The five security goals are integrity, availability, confidentiality, accountability, and assurance.

Security incident—Any act or circumstance that involves classified information that deviates from the requirements of governing security publications. For example, compromise, possible compromise, inadvertent disclosure, and deviation.

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

Security kernel—The central part of a computer system (hardware, software, or firmware) that implements the fundamental security procedures for controlling access to system resources.

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

Security metrics—A standard of measurement used to measure and monitor information security-related information security activity.

Security objective—Confidentiality, integrity, or availability of information.

Security Parameter Index (SPI)—SPI is an identifier for a security association within a specific security protocol. This means that a pair of security protocol and SPI may uniquely identify a security association, but this is implementation dependent.

Security plan—See system security plan.

Security policy—The set of laws, rules, and practices that regulate how sensitive or critical information is managed, protected, and distributed. .

Security policy model—A formal presentation of the security policy enforced by the system. It must identify the set of rules and practices that regulate how a system manages, protects, and distributes sensitive information.

Security process—The series of activities that monitor, evaluate, test, certify, accredit, and maintain the system accreditation throughout the system life cycle.

Security program—A systems program that controls access to data in files and permits only authorized use of terminals and other related equipment. Control is usually exercised through various levels of safeguards assigned on the basis of the user's need-to-know.

Security purpose—The IS security purpose is to provide value by enabling an organization to meet all mission/business objectives while ensuring that system implementations demonstrate due care consideration of risks to the organization and its customers.

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

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

Security service—A capability that supports one, or many, of the security goals. Examples of security services are key management, access control, and authentication.

Security specification—A detailed description of the safeguards required to protect a system.

Security Test and Evaluation (ST&E)—An examination and analysis of the security safeguards of a system as they have been applied in an operational environment to determine the security posture of the system.

Security testing—A process used to determine that the security features of a system are implemented as designed. This includes hands-on functional testing, penetration testing, and verification.

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.

Seepage—The accidental flow, to unauthorized individuals, of data or information that is presumed to be protected by computer security safeguards.

Segment—Under HIPAA, this is a group of related data elements in a transaction. Also see Part II, 45 CFR162.103.

SEL—Security audit event selection.

Selection—A program control structure created in response to a condition test in which one of two or more processing paths can be taken.

Self sourcing (or knowledge worker/end-user development)—The development and support of IT systems by knowledge workers with little or no help from IT specialists.

Self-insured—Under HIPAA, an individual or organization that assumes the financial risk of paying for healthcare.

Self-organizing neural network—A network that finds patterns and relationships in vast amounts of data by itself.

Selling prototype—A prototype used to convince people of the worth of a proposed system.

Semagram—meaning: semantic symbol. Semagrams are assoicated with a concept and do not use writing to hide a message.

Semiconductor —Material used in electronic components that possesses electrical conducting qualities of conductors and resistors.

Sensitive data—Data that is considered confidential or proprietary. The kind of data that, if disclosed to a competitor, might give away an advantage.

Sensitive information—Any information that requires protection and that should not be made generally available.

Sensitive Intelligence Information—Such intelligence information, the unauthorized disclosure of which would lead to counteraction (1) jeopardizing the continued productivity of intelligence sources or methods which provide intelligence vital to the national security; or (2) offsetting the value of intelligence vital to the national security.

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

Sensitivity—An information technology environment consists of the system, data, and applications, which must be examined individually and in total. All systems and applications require some level of protection for confidentiality, integrity, and availability. This level of protection is determined by an evaluation of the sensitivity and criticality of the information processed, the relationship of the system to the organization’s mission, and the economic value of the system components. .

Sensitivity attributes—User-supplied indicators of file sensitivity that the system uses to enforce an access control policy.

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.

SEP—Protection of the TSF, domain separation.

Sequential organization—The physical arrangement of records in a sequence that corresponds with their logical key.

Serial connector—Usually has 9 holes but may have 25 that fit into the corresponding number of pins in the port. Serial connectors are often used for monitors and certain types of modems.

Serial Line Internet Protocol (SLIP)—An Internet protocol used to run IP over serial lines such as telephone circuits or RS-232 cables interconnecting two systems. SLIP is now being replaced by Point-to-Point Protocol. *See* Point-to-Point Protocol.

Serial Line IP (SLIP)—An IP used to run over serial lines such as telephone circuits or RS-232 cables interconnecting two systems. SLIP is now being replaced by Point-to-Point Protocol. See Point-to-Point Protocol.

Serial organization—The physical arrangement of records in a sequence.

Serial processing—The processing of records in the physical order in which they appear in a file or on an input device.

Server—A computer that provides a service to another computer, such as a mail server, a file server, or a news server.

Server farm—A location that stores a group of servers in a single place.

Service—A component of the portfolio of choices offered by SvPs to a user, a functionality offered to a user.

Service control—The ability of the user, home environment, or serving environment to determine what a particular service does, for a specific invocation of that service, within the limitations of that service.

Service Control Points (SCP)—The local versions of the national 800 number database. They contain the intelligence to screen the full ten digits of an 800 number and route calls to the appropriate long distance carrier.

Service information—Information used by the telecommunications infrastructure in the establishment and operation of a network-related service or services. The information may be established by an NWO/AP/SvP or a network user.

Service Level Agreement (SLA)—Defines the specific responsibilities of the service provider and sets the customer expectations.

Service program—An operating system program that provides a variety of common processing services to users (e.g., utility programs, librarian programs, and other software).

Service Provider (SvP)—A natural or legal person providing one or more public telecommunications services whose provision consists wholly or partly in the transmission and routing of signals on a telecommunications network. SvPs do not necessarily have to run their own networks.

Service Switching Points (SSP)—A switching system, including its remotes, that identifies calls associated with intelligent network services and initiates dialog with the SCP.

Service Transfer Points (STP)—A signaling point with the function of transferring messages from one signaling link to another and considered exclusively from the viewpoint of the transferor.

Session—A completed connection to an Internet service, and the ensuing connect time.

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

Session key—Session key is a randomly-generated key that is used one time, and then discarded. Session keys are symmetric (used for both encryption and decryption). They are sent with the message, protected by encryption with a public key from the intended recipient. A session key consists of a random number of approximately 40 to 2000 bits. Session keys can be derived from hash values.

Session layer—The layer of the ISO Reference Model coordinating communications between network nodes. It can be used to initialize, manage, and terminate communication sessions.

SET—Secure Electronic Transactions protocol.

SF—Super Framing (T1/E1).

SHA—Secure Hash algorithm.

Shared information—An organization's information is in one central location allowing anyone to access and use it as they need it.

Shareware—Software available on the Internet that may be downloaded to your machine for evaluation and for which you are generally expected to pay a fee to the originator of the software if you decide to keep it.

Sharing—Providing access to and facilitating the sharing of information which enhances reach and creates shared awareness.

Shortfalls—Functional areas in which additional capability or coverage is required.

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

Sign a message—To use your private key to generate a digital signature as a means of proving you generated, or certify, some message.

Signaling—The exchange of information specifically concerned with the establishment and control of connections, and with management, in a telecommunications network.

Signaling System 7 (SS7)—SS7 employs a dedicated 64-kb data circuit to carry packetized machine language messages about each call connected between and among machines of a network to achieve connection control.

Signal-to-Interference Ratio (SIR)—The ratio of the usable signal being transmitted to the noise or undesired signal.

Signature (digital)—A quantity (number) associated with a message which only someone with knowledge of your private key could have generated, but which can be verified through knowledge of your public key.

Signature dynamics—A form of electronic signatures which involves the biometric recording of the pen dynamics used in signing the document.

Sign-off—The knowledge workers' actual signatures indicating they approve all of the business requirements.

SIL—Safety integrity level.

SIMM—Single inline memory module.

Simple Mail Transfer Protocol (SMTP)—The Internet e-mail protocol.

Simple Network Management Protocol (SNMP)—Provides remote administration of network device; "simple" because the agent requires minimal software.

Simplicity—The simplest correct structure is the most desirable.

Simulation—The use of an executable model to represent the behavior of an object. During testing, the computational hardware, the external environment, and even the coding segments may be simulated.

Simultaneous processing—The execution of two or more computer program instructions at the same time in a multiprocessing environment.

Single inheritance—The language mechanism that allows the definition of a class to include the attributes and methods defined for, at most, one superclass.

Single sideband carrier—An amplitude modulation technique for encoding analog or digital data using either analog or digital transmission. Single sideband suppresses one sideband of the carrier frequency at the source. As such, less power is used, and less bandwidth is required.

SIP—SMDS Interface Protocol.

Site—An immobile collection of systems at a specific location.

Site accreditation—An accreditation where all systems at a location are grouped into a single management entity. A DAA may determine that a site accreditation approach is optimal given the number of information technology systems, major applications, networks, or unique operational characteristics. Site accreditation begins with all systems and their interoperability and major applications at the site being certified and accredited. The site is then accredited as a single entity, and an accreditation baseline is established.

Situation—Situation is a set of all security-relevant information. The decision of an entity on which security services it requires is based on the situation.

Skill words—Nouns and adjectives used by organizations to describe job skills that should be woven into the text of applicants' resumes.

Skin affect—The concept that high-frequency energy travels only on the outside skin of a conductor and does not penetrate into it any great distance.

Slack space—The unused space in a group of disk sectors. Or the difference in empty bytes of the space that is allocated in clusters minus the actual size of the data files. .

SLARP—Serial Link Address Resolution Protocol.

Slave computer—A front-end processor that handles input and output functions for a host computer.

SLDC (1)—Systems development life cycle.

SLDC (2)—Synchronous Data Link Control.

SLIP—Serial Line Interface Protocol.

Small Health Plan—Under HIPAA, this is a health plan with annual receipts of $5 million or less. Also see Part II, 45 CFR 160.103.

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

SMDS—Switched Multi-megabit Data Service.

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.

SMR—Security management, security management roles.

SMTP—Simple Mail Transfer Protocol.

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

SNA—Systems Network Architecture.

SNAP—Subnetwork Access Protocol.

SNF— Skilled Nursing Facility.

Sniffing—An attack capturing sensitive pieces of information, such as a password, passing through the network.

SNIP—Strategic National Implementation Process--Sponsored by WEDI.

SNMP—Simple Network Management Protocol.

SNOMED—Under HIPAA, Systematized Nomenclature of Medicine.

Sociability—The ability of intelligent agents to confer with each other.

Social engineering—An attack based on deceiving users or administrators at the target site. For example, a person who illegally enters computer systems by persuading an authorized person to reveal IDs, passwords and other confidential information.

Socket—A paring of an IP address and a port number. *See* port.

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. Compare with *SML.*

Softlifting—Illegal copying of licensed software for personal use.

Software—Computer programs, procedures, rules, and possibly documentation and data pertaining to the operation of the computer system.

Software integrity level—The integrity level of a software item.

Software life cycle—The period of time beginning when a software product is conceived and ending when the product is no longer available for use. The software life cycle is typically broken into phases (e.g., requirements, design, programming, testing, conversion, operations, and maintenance).

Software maintenance—All changes, corrections, and enhancements that occur after an application has been placed into production.

Software piracy—To illegally copy software.

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.

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.

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.

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.

Software suite—Bundled software that comes from the same publisher and costs less than buying all the software pieces individually.

SONET—Synchronous Optical Network.

SOP—Standard operating procedure.

Sort—The arrangement of data in ascending or descending, alphabetic or numeric order.

SOS—Identification and authentication specification of secrets.

Source document—The form that is used for the initial recording of data prior to system input.

Source program—The computer program that is coded in an assembler or higher-level programming language.

SOW—See *Statement of Work.*

Space diversity—Protection of a radio signal by providing a separate antenna located a few feet below the regular antenna on the same tower to assume the load when the regular transmission path on the tower fades.

Space Division Multiple Access (SDMA)—Intelligent antenna systems use this access method to increase the capacity of cellular radio networks by separating frequencies within a cell site and allowing the same frequencies to be reused.

Spam—The act of posting the same information repeatedly on inappropriate places or too many places so as to overburden the network.

Spam—Unsolicited e-mail.

Spam filters—Programs that detect and reject spam by looking for certain keywords, phrases or Internet addresses. .

Spatial domain—the image plane itself; the collection of pixels that composes an image.

Special agent—A special agent in the Diplomatic Security Service (DSS) is a sworn officer of the Department of State or the Foreign Service, whose position is designated as either a GS-1811 or FS-2501, and has been issued special agent credentials by the Director of the Diplomatic Security Service to perform those specific law enforcement duties as defined in 22 U.S.C. 2712.

Special investigators—Special investigators are contracted by the Department of State. They perform various noncriminal investigative functions in DS headquarters, field, and resident offices. They are not members of the Diplomatic Security Service and are not authorized to conduct criminal investigations.

Specification—A description of a problem or subject that will be implemented in a computational or other system. The specification includes both a description of the subject and aspects of the implementation that affect its representation. Also, the process and analysis and design that results in a description of a problem or subject that can be implemented in a computation or other system.

Spectrum—The radio frequency that is available for personal, commercial, and military use.

SPF—Shortest Path First.

Spherical zone of control—A volume of space in which uncleared personnel must be escorted which extends a specific distance in all directions from TEMPEST equipment processing classified information or from a shielded enclosure.

SPI—Security parameter index; part of IPSec.

SPID—Service Provider Identifier (ISDN).

Split knowledge—A security technique in which two or more entities separately hold data items that individually convey no knowledge of the information that results from combining the items. A condition under which two or more entities separately have key components which individually convey no knowledge of the plaintext key that will be produced when the key components are combined in the cryptographic module.

SPM—Development, security policy modeling.

Sponsor—See Plan Sponsor.

Spoof—To make a transmission appear to come from a user other than the user who performed the action. .

Spoofing—1. Faking the sending address of a transmission to gain illegal entry into a secure system. 2. The deliberate inducement of a user or resource to take incorrect action.

Spooling—A technique that maximizes processing speed through the temporary use of high-speed storage devices. Input files are transferred from slower, permanent storage and queued in the high-speed devices to await processing, or output files are queued in high-speed devices to await transfer to slower storage devices.

SPP—Sequenced Packet Protocol (Vines).

Spread spectrum image steganography—A method of steganographic communication that uses digital imagery as the cover signal.

Spread spectrum techniques—The method of hiding a small or narrow-band signal (message) in a large or wide band cover.

Spreadsheet software—Computer software that divides a display screen into a large grid. This grid allows the user to enter labels and values that can be manipulated or analyzed.

Spread-spectrum image steganography—A method of steganographic communication that uses digital imagery as the cover signal.

Spread-spectrum techniques—The method of hiding a small or narrow-band signal (message) in a large or wideband cover. **.**

SPX—Sequenced Packet Exchange (Novell).

Spyware—Any software that covertly gathers user information through the user's Internet connection without his or her knowledge, usually for advertising purposes. Spyware applications are typically bundled as a hidden component of freeware or shareware programs that can be downloaded from the Internet; however, it should be noted that the majority of shareware and freeware applications do not come with spyware. Once installed, the spyware monitors user activity on the Internet and transmits that information in the background to someone else. Spyware can also gather information about e-mail addresses and even passwords and credit card numbers. Also known as *adware.*

SQL—See *Structured Query Language.*

SRAM—Static RAM.

SRB—Source route bridging.

SRE—(1) Protection Profile evaluation, explicitly stated IT security requirements; (2) Security Target evaluation, explicitly stated IT security requirements.

SRTB—Source route transparent bridging.

SRTP—Sequenced Routing Update Protocol (Vines).

SS7—Signaling System 7.

SSAP—Source Service Access Point (LLC).

SSH—Secure Shell.

SSL—Secure Sockets Layer.

SSL3—Secure Socket Layer protocol; see also TLS1.

SSN—Social Security number.

SSO—Single Sign-On *or* Standards Setting Organization.

SSO—See *Standard-Setting Organization.*

SSP—In Common Criteria, protection of the TSF, state synchrony protocol.

ST—Security target.

Stacked-job processing—A computer processing technique in which programs and data awaiting processing are placed into a queue and executed sequentially.

Standalone root—A certificate authority that signs its own certificates and does not rely of a directory service to authenticate users.

Standard—Mandatory statement of minimum requirements that support some part of a policy.

Standard Generalized Markup Language (SGML)—An international standard for encoding textual information that specifies particular ways to annotate text documents separating the structure of the document from the information content. HTML is a generalized form of SGML.

Standard transaction—Under HIPAA, this is a transaction that complies with the applicable HIPAA standard. Also see Part II, 45 CFR 162.103.

Standard Transaction Format Compliance System (STFCS)—An EHNAC-sponsored WPC-hosted HIPAA compliance certification service.

Standardization—The commander's information requirements must not be comprised by the use of nonstandard equipment.

Standards—A set of rules or specifications that, when taken together, define a software or hardware device. A standard is also an acknowledged basis for comparing or measuring something. Standards are important because new technology will only take root once a group of specifications is agreed upon.

Standards audit—The check to ensure that applicable standards are properly used.

Standard-Setting Organization (SSO)—See Part II, 45 CFR 160.103.

State—A static condition of an object or group of objects.

State space—The total collection of possible states for a particular object or group of objects.

State transition—A change of state for an object; something that can be signaled by an event.

State Uniform Billing Committee (SUBC)—Under HIPAA, a state-specific affiliate of the NUBC.

State variable—A property or type that is part of an identified state of a given type.

Statement of Work (SOW)—Under HIPAA, a document describing the specific tasks and methodologies that will be followed to satisfy the requirements of an associated contract or MOU.

Statement testing—A test method of satisfying the criterion that each statement in a program be executed at least once during the program testing.

Static analysis—The direct analysis of the form and structure of a product that does not require its execution. It can be applied to the requirements, design, or code.

Static data—Data that, once established, remains constant.

Statistical Time Division Multiplexing (STDM)—This form of multiplexing uses all available time slots to send significant information and handles inbound data on a first-come, first-served basis.

Steering committee—A management committee assembled to sponsor and manages various projects such as information security program.

Steganalysis—The art of detecting and neutralizing steganographic messages.

Steganalyst—One who applies steganalysis with the intent of discovering hidden information.

Steganographic file system—A method of storing files in such a way that encrypts data and hides it such that it cannot be proven to be there.

Steganography—(1) The method of concealing the existence of a message or data within seemingly innocent covers. (2) A technology used to embed information in audio and graphical material.

The audio and graphical materials appear unaltered until a steganography tool is used to revel the hidden message.

Stegokey—A key that allows extraction of the secret information out of the cover.

Stego-medium—The resulting combination of a cover medium and embedded message and a stego key. .

Stego-only attack—An attack where only the stego-object is available for analysis.

STFCS—See the Standard Transaction Format Compliance System.

STG—Security audit event storage.

StirMark—A method of testing the robustness of a watermark. StirMark is based on the premise that many watermarks can survive a simple manipulation to the file, but not a combination of manipulations. It simulates a process similar to what would happen if an image was printed and then scanned back into the computer by stretching, shearing, shifting and rotating an image by a tiny random amount.

STM—Protection of the TSF, time stamps.

Storage media—Floppy diskettes, tapes, hard disk drives, or any devices that store automated information.

Storage object—An object that supports both read and write accesses.

Stored-program concept—The location of the instructions placed in the memory of a common controlled switching unit and to which it refers while processing a call.

Strategic management—Provides an organization with overall direction and guidance.

Strategic National Implementation Process (SNIP)—Under HIPAA, a WEDI program for helping the healthcare industry identify and resolve HIPAA implementation issues.

Stream cipher—An encryption method in which a cryptographic key and an algorithm are applied to each bit in a datastream, one bit at a time.

Strength—The power of the information assurance protection.

Strength of Mechanism (SML)—A scale for measuring the relative strength of a security mechanism hierarchically ordered from SML 1 through SML 3.

Strike warfare—A primary warfare mission area dealing with preemptive or retaliatory offensive strikes against inland or coastal ground targets.

Strong authentication—Strong authentication refers to systems that require multiple factors for authentication and use advanced technology, such as dynamic passwords or digital certificates, to verify a user's identity.

Structurally object-oriented—[The data model allows definitions of data structures to represent entities of any complexity (complex objects).

Structured data—See *Data-Related Concepts.*

Structured design—A methodology for designing systems and programs through a top-down, hierarchical segmentation.

Structured programming—The process of writing computer programs using logical, hierarchical control structures to carry out processing.

Structured Query Language (SQL)—The international standard language for defining and accessing a relational database.

SUBC—See *State Uniform Billing Committee.*

Subject—An active entity, generally in the form of a person, process, or device that causes information to flow among objects or changes the system state.

Subjective information—Attempts to describe something that is unknown.

Subnet—A portion of a network, which may be a physically independent network segment, that shares a network address with other portions of the network and is distinguished by a subnet number. A subnet is to a network what a network is to the Internet.

Subnet address—The subnet portion of an IP address. In a subnetted network, the host portion of an IP address is split into a subnet and a host portion using an address (subnet) mask.

Subroutine—A segment of code that can be called up by a program and executed at any time from any point.

Subscriber—An entity (associated with one or more users) that is engaged in a subscription with a telecommunications service provider (TSP). The subscriber is allowed to subscribe to and unsubscribe from services, to register a user or a list of users authorized to enjoy these services, and also to set the limits relative to the use that associated users make of these services.

Subscriber loop—The circuit that connects the telephone company's central office to the demarcation point on the customer's premises. The circuit is most likely a pair of wires.

Subscript—A value used in programming to reference an item of data stored in a table.

Substitution—the steganographic method of encoding information by replacing insignificant bits from the cover with the bits from the embedded message.

Substitution-Linear Transformation Network—A practical architecture based on Shannon's concepts for the secure, practical ciphers with a network structure consisting of a sequence of rounds of small substitutions, easily implemented by table lookup and connected by bit position permutations or linear transpositions.

Subsystem—A major subdivision or component of an information system consisting of information, information technology, and personnel that performs one or more specific functions. .

Suite—A named set of resources and interfaces; a collection of resources; not a physical space.

Summary Health Information—See Part II, 45 CFR 164.504.

Superclass—A class from which another class inherits attributes and methods.

Supercomputer—The fastest, most powerful, and expensive type of computer.

SuperFrame—A synchronization-framing format for a T1. In a T1 circuit, each of the 24 DS0 channels are sampled every 125 microseconds and 8 bits are taken from each. If you multiply the 8 bits by the 24 channels, you get 192-bits in a chain, and then add one bit for timing, you get 193 total bits in one frame. Twelve frames comprise the SuperFrame. A newer version of this T1 formatting is called Extended Super Frame (ESF).

Supply chain—The paths reaching out to all of a company's suppliers of parts and services.

Supply-Chain Management (SCM) system—Tracks inventory and information among business processes and across companies.

Support Mission Area—Synonymous with Support Warfare Mission Area. Areas of Naval warfare that provide support functions that cut across the boundaries of all (or most) other warfare mission areas.

Supraliminal channel—a feature of an image which is impossible to remove without gross modifications, i.e.--a visible watermark.

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

SVC—Switched virtual circuit.

Swapping—A method of computer processing in which programs not actively being processed are held on special storage devices and alternated in and out of memory with other programs according to priority.

SWG—Under HIPAA, sub-workgroup.

Switch—A mechanical, electrical, or electronic device that opens or closes circuits, completes or breaks an electrical path, or selects paths or circuits. A switch looks at incoming data to determine the destination address. Based on that address, a transmission path is set up through the switching matrix between the incoming and outgoing physical communications ports and links.

Switch Control Point (SCP) also known as Service Control Point (SCP)—Provides computer services, such as database information, that defines the possible services and their logic.

Switched beam—Also called switch lobe. Smart antennas use power patterns that are more concentrated and directed than the regular antenna. The far end device receives a much more powerful signal from the antenna.

Switched Lobe (SL)—Also called switch beam. Smart antennas use power patterns that are more concentrated and directed than the regular antenna. The far end device receives a much more powerful signal from the antenna.

Switched Virtual Circuit (SVC)—A virtual circuit connection established across a network on an as-needed basis and lasting only for the duration of the transfer.

Switching costs—Costs that can make customers reluctant to switch to another product or service.

Symbolic evaluation—The process of analyzing the path of program execution through the use of symbolic expressions.

Symbolic execution—The analytical technique of dissecting each program path.

Symmetric key encryption—In symmetric key encryption: two trading partners share one or more secrets, no one else can read their messages. A different key (or set of keys) is needed for each pair of trading partners. Same key used for encryption and decryption.

Synchronous—A protocol of transmitting data over a network where the sending and receiving terminals are kept in synchronization with each other by a clock signal embedded in the data.

Synchronous Optical NETwork (SONET)—SONET is an international standard for high-speed data communications over fiber-optic media. The transmission rates range from 51.84 Mbps to 2.5 Gbps.

Syntax—The statement formats and rules for the use of a programming language.

System—A series of related procedures designed to perform a specific task.

System accreditation—The official authorization granted to an information system to process sensitive information in its operational environment based on a comprehensive security evaluation of the system's hardware, firmware, and software security design, configuration and implementation and of the other system procedural, administrative, physical, TEMPEST, personnel, and communications security controls.

System analysis—The process of studying information requirements and preparing a set of functional specifications that identify what a new or replacement system should accomplish.

System attributes—The qualities, characteristics, and distinctive features of information systems.

System bus—The electronic pathways that move information between basic components on the motherboard, including the pathway between the CPU and RAM.

System certification—The technical evaluation of a system's security features that established the extent to which a particular information system's design and implementation meets a set of specified security requirements.

System design—The development of a plan for implementing a set of functional requirements as an operational system.

System development life cycle—The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and, ultimately, its disposal, which instigates another system initiation. .

System entity—A system subject (user or process) or object.

System environment—the unique technical and operating characteristics of an IT system and its associated environment, including the hardware, software, firmware, communications capability, organization, and physical location.

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.

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 processed (including all compartments and special access programs); and c. Valid need-to-know for some of the information contained within the IS.

System integrity—The 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 integrity procedures—Procedures established to ensure that hardware, software, firmware, and data in a computer system maintain their state of original integrity and are not tampered with by unauthorized personnel.

System interconnection—The direct connection of two or more information technology systems for the purpose of sharing data and other information resources.

System log—An audit trail of relevant system happenings (e.g., transaction entries, database changes).

System owner—Official having responsibility for the overall procurement, development, integration, modification, or operation and maintenance of an information system. .

System reliability—The composite of hardware and software reliability for a specified operational environment. System reliability measurements combine qualitative and quantitative assessments.

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.

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.

System Security Authorization Agreement (SSAA)—The SSAA is a formal agreement among the DAA(s), the Certifier, user representative, and program manager. It is used throughout the entire DITSCAP to guide actions, document decisions, specify IA requirements, document certification tailoring and level-of-effort, identify potential solutions, and maintain operational systems security.

System security plan—Formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements. .

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.

System test—The process of testing an integrated hardware/software system to verify that the system meets its specified requirements.

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

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

Systems analysis—The process of studying information requirements and preparing a set of functional specifications that identify what a new or replacement system should accomplish.

Systems architecture—The fundamental and unifying system structure defined in terms of system elements, interfaces, processes, constraints, and behaviors.

Systems design—The development of a plan for implementing a set of functional requirements as an operational system.

Systems Development Life Cycle (SDLC)—(1) The classical operational development methodology that typically includes the phases of requirements gathering, analysis, design, programming, testing, integration, and implementation. (2) The systematic systems building process consisting of specific phases; for example, preliminary investigation, requirements determination, systems analysis, systems design, systems development, and systems implementation.

Systems engineering—An integrated composite of people, products, and processes that provides a capability or satisfies a stated need or objective.

Systems Network Architecture (SNA)—IBM's proprietary network architecture.

Systems security—There are three parts to Systems Security: (1) Computer Security (COMPUSEC) is composed of measures and controls that protect an AIS against denial-of-service, unauthorized disclosure, modification, or destruction of AIS and data (information). (2) Communications Security (COMSEC) is measures and controls taken to deny unauthorized persons information derived from telecommunications of the U.S. government. Government communications regularly travel by computer networks, telephone systems, and radio calls. (3) Information Systems Security (INFOSEC) is controls and measures taken to protect telecommunications systems, automated information systems, and the information they process, transmit, and store.

Systems software—The programs and other processing routines that control and activate the computer hardware facilitating its use.

System-specific security control—A security control for an information system that has not been designated as a common security control. .

T-1—Trunk Level 1. A digital transmission link with a total signaling speed of 1.544 Mbps.

TA—Terminal adapter.

TA/NT1TCB—Terminal Adapter/Network Termination 1 (ISDN) Trusted Computing Base.

TAB—TOE access, TOE access banners.

Table—An area of computer memory containing multiple storage locations that can be referenced by the same name.

Table driven—An indexed file in which tables containing record keys (i.e., disk addresses) are used to retrieve records.

TACACS (Terminal Access Controller Access Control System)—Authentication protocol, developed by the DDN community that provides remote access authentication and related services, such as event logging. User passwords are administered in a central database rather than in individual routers, providing an easily scalable network security solution.

TACACS+—Terminal Access Controller Access Control System Plus is an authentication protocol, often used by remote-access servers or single (reduced) sign-on implementations. TACACS and TACACS+ are proprietary protocols from CISCO®.

Tactical management—Develops the goals and strategies outlined by strategic management.

TAG—Under HIPAA, Technical Advisory Group.

TAH—TOE access, TOE access history.

Tampering—An intentionally caused event that results in modification of a system, its intended behavior, or data.

Tandem switch—A tandem switch connects one trunk to another. An intermediate switch or connection between an originating telephone call location and the final destination of the call. The tandem point passes the call along.

Tape management system—Systems software that assesses the given information on jobs to be run and produces information for operators and librarians regarding which data resources (e.g., tapes and disks) are needed for job execution.

Target identification—Identity that relates to a specific lawful authorization as such. This may be a serial number or a combination of characters and numbers. It is not related to the denoted interception subject or subjects.

Target identity—The identity associated with a target service used by the interception subject.

Target of Evaluation (TOE)—Under Common Criteria, an IT product or system that is subject to an evaluation.

Target service—Telecommunications service associated with an interception subject and usually specified in a lawful authorization for interception. There may be more than one target service associated with a single interception subject.

Task management system—It allocates the processor unit resources according to priority scheme or other assignment methods.

TAT—Lifecycle support, tools and techniques.

TCB—Trusted computing base.

TCP—Transport Control Protocol.

TCP sequence prediction—Fools applications using IP addresses for authentication (like the UNIX rlogin and rsh commands) into thinking that forged packets actually come from trusted machines.

TCP/IP—Transmission Control Protocol/Internet Protocol is a set of communications protocols that encompasses media access, packet transport, session communications, file transfer, electronic mail, terminal emulation, remote file access and network management. TCP/IP provides the basis for the Internet. The structure of TCP/IP is as follows:
Process layer clients: FTP, Telnet, SMTP, NFS, DNS:
Transport layer service providers: TCP (FTP, Telnet, SMTP), UDP (NFS, DNS): Network layer: IP (TCP, UDP): Access layer: Ethernet (IP), Token ring (IP).

TCSEC—Trusted Computer Systems Evaluation Criteria.

TDC—In Common Criteria, protection of the TSF: inter-TSF TSF data consistency.

TDM—Time division multiplexing.

TE—Terminal equipment.

TE1 and TE2—Terminal endpoints.

Technical architecture—Defines the hardware, software, and telecommunications equipment required to run the system.

Technical certification—A formal assurance by the Undersecretary for Management to Congress that standards are met which apply to an examination, installation, test or other process involved in providing security for equipment, systems, or facilities. Certifications may include exceptions and are issued by the office or person performing the work in which the standards apply.

Technical controls—The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.

Technical penetration—An unauthorized RF, acoustic, or emanations intercept of information. This intercept may occur along a transmission path which is (1) known to the source, (2) fortuitous and unknown to the source, or (3) clandestinely established.

Technical steganography—The method of steganography where a tool, device or method is used to conceal a message. *Example:* invisible inks and microdots .

Technical surveillance—The act of establishing a technical penetration and intercepting information without authorization.

Technological attack—An attack that can be perpetrated by circumventing or nullifying hardware, software, and firmware access control mechanisms rather than by subverting system personnel or other users.

Technology-literate knowledge worker—A person who knows how and when to apply technology.

Telecommunications—Any transmission, emission, or reception of signs, signals, writing, images, sounds, or other information by wire, radio, visual, satellite, or electromagnetic systems.

Telecommunications carrier—An entity engaged in the transmission or switching of wire or electronic communications as a common carrier for hire that:.

Telecommunications device—A tool used to send information to and receive it from another person or location.

Telecommunications service—The offering of telecommunications for a fee directly to the public or to such classes of users as to be effectively available directly to the public, regardless of the facilities used.

Telecommunications Service Provider (TSP)—Umbrella term for APs, SPs, SvPs, and NWOs.

Telecommunications Standardization Sector of the International Telecommunications Union (ITU-TSS)—A unit of the International Telecommunications Union (ITU) of the United Nations. An organization with representatives from the post office, telegraph, and telecommunications agencies (PTTs) of the world. ITU-TSS produces technical standards, known as recommendations, for all internationally controlled aspects of analog and digital communications.

Telecommuting—The use of communications technologies (such as the Internet) to work in a place other than a central location.

Teleprocessing—Information processing and transmission performed by an integrated system of telecommunications, computers, and person-to-machine interface equipment.

Teleprocessing security—The protection that results from all measures designed to prevent deliberate, inadvertent, or unauthorized disclosure or acquisition of information stored in or transmitted by a teleprocessing system.

Telnet—The virtual terminal protocol in the Internet suite of protocols. Allows users of one host to log into a remote host and interact as normal terminal users of that host.

TEMPEST—The study and control of spurious electronic signals emitted from electronic equipment. TEMPEST is a classification of technology designed to minimize the electromagnetic emanations generated by computing devices. TEMPEST technology makes it difficult, if not impossible, to compromise confidentiality by capturing emanated information.

TEMPEST Certification—Nationally approved hardware that protects against the transmission of compromising emanations, i.e., unintentional signals from information processing equipment which can disclose information being processed by the system.

TEMPEST Equipment (or TEMPEST-Approved Equipment)—Equipment that has been designed or modified to suppress compromising signals. Such equipment is approved at the national level for U.S. classified applications after undergoing specific tests. National TEMPEST approval does not, of itself, mean a device can be used within the foreign affairs community. Separate DS approval is required.

TEMPEST Hazard—A security anomaly that holds the potential for loss of classified information through compromising emanations.

TEMPEST Test—A field or laboratory examination of the electronic signal characteristics of equipment or systems for the presence of compromising emanations.

TEMPEST-Approved Personal Computer (TPC)—A personal computer that is currently listed on the Preferred Products List (PPL) or Evaluated Products List (EPL).

Temporal masking—A form of masking that occurs when a weak signal is played immediately after a strong signal. .

Temporary advantage—An advantage that, sooner or later, the competition duplicates or leap frogs with a better system.

Tenant Agency—A U.S. government department or agency operating overseas as part of the U.S. foreign affairs community under the authority of a chief of mission. Excluded are military elements not under direct authority of the chief of mission.

Terabyte (TB)—Roughly 1 trillion bytes.

Terminal identification—The means used to establish the unique identification of a terminal by a computer system or network.

Test condition—A detailed step the system must perform along with the expected result of the step.

Test Data—Data that simulates actual data to form and content and is used to evaluate a system or program before it is put into operation.

Test data generators—Computer software tools that help generate files of data that can be used to test the execution and logic of application programs.

Testing—The examination of the behavior of a program through its execution on sample data sets.

Texture block coding—A method of watermarking that hides data within the continuous random texture patterns of an image. The technique is implemented by copying a region from a random texture pattern found in a picture to an area that has similar texture, resulting in a pair of identically textured regions in the picture. .

TFTP—Trivial File Transfer Protocol.

TG—Under HIPAA, Task Group.

The Prisoner's Problem—A model for steganographic communication.

Thin client—A workstation with a small amount of processing power and costing less than a full-powered workstation.

Third-party ad servers—Companies that display banner advertisements on Web sites that you visit. These companies are often not the ones that own the Web site. .

Third-Party Administrator (TPA)—Under HIPAA, an entity that processes healthcare claims and performs related business functions for a health plan.

Threat—The potential danger that a vulnerability may be exploited intentionally, triggered accidentally, or otherwise exercised.

Threat agent—A means or method used to exploit a vulnerability in a system, operation, or facility.

Threat analysis—A project to identify the threats that exist over key information and information technology. The threat analysis usually also defines the level of the threat and likelihood of that threat to materialize.

Threat assessment—Process of formally evaluating the degree of threat to an information system and describing the nature of the threat.

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 monitoring—The analysis assessment and review of audit trails and other data collected to search out system events that may constitute violations or precipitate incidents involving data privacy.

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

Threat source—Either (1) intent and method targeted at the intentional exploitation of a vulnerability or (2) the situation and method that may accidentally trigger a vulnerability.

Three generic strategies—Cost leadership, differentiation, and a focused strategy.

Three-dimensional (3D) technology—Presentations of information that give the user the illusion that the object viewed is actually in the room with the user.

Three-Way Handshake—The process whereby two protocol entities synchronize during connection establishment.

Thrill-seeker hacker—A hacker who breaks into computer systems for fun.

Throughput—The process of measuring the amount of work a computer system can handle within a specified timeframe.

TIFF—Tagged Image Format.

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

Time Division Multiple Access (TDMA)—One of several technologies used to separate multiple conversation transmissions over a finite frequency allocation of through-the-air bandwidth. TDMA is used to allocate a discrete amount of frequency bandwidth to each user in order to permit many simultaneous conversations. However, each caller is assigned a specific time slot for transmission.

Time Division Multiplexing (TDM)—A technique for transmitting a number of separate data, voice, and video signals simultaneously over one communications medium by interleaving a piece of each signal one after another.

Time domain—Method of representing a signal where the vertical deflection is the signals amplitude, and the horizontal deflection is the time variable.

Time stamping—An electronic equivalent of mail franking.

Time-Dependent Password—A password that is valid only at a certain time of day or during a specified timeframe.

Timeliness—The ability to ensure the delivery of required information within a defined time frame. Availability of required information in time to make decisions and permit execution within an adversary's decision and execution cycle.

Timely—[JITC, 1999]: In-time, reasonable access to data or system capabilities.

Timestamping—The practice of tagging each record with some moment in time, usually when the record was created or when the record was passed from one environment to another.

Tip side—Side of the line when measured with a voltmeter to an earth ground that should read zero voltage.

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—Under Common Criteria, target of evaluation.

TOE Security Functions (TSF)—Under Common Criteria, all parts of the TOE that have to be relied upon for enforcement of the TSP.

TOE Security Policy (TSP)—Under Common Criteria, the rules defining the required security behavior of a TOE. .

Token passing—A network access method that uses a distinctive character sequence as a symbol (token), which is passed from node to node, indicating when to begin transmission. Any node can remove the token, begin transmission, and replace the token when it is finished.

Token ring—A type of area network in which the devices are arranged in a virtual ring in which the devices use a particular type of message called a token to communicate with one another.

Top-level domain—Three-letter extension of a Web site address that identifies its type.

Total risk—The potential for the occurrence of an adverse event if no mitigating action is taken (i.e., the potential for any applicable threat to exploit a system vulnerability). See also *acceptable risk, residual risk*, and *minimum level of protection*.

Touch screen—Special screen the user touches to perform a particular function.

Touchpad—Popular on notebook computers, a stationary mouse that is touched with the finger.

TPA—See Third-Party Administrator or Trading Partner Agreement.

Traceroute—(1) A program available on many systems that traces the path a packet takes to a destination. It is mostly used to debug routing problems between hosts. There is also a traceroute protocol defined in RFC 1393. (2) The traceroute or finger commands to run on the source machine (attacking machine) to gain more information about the attacker.

Trackball—An upside-down, stationary mouse in which the ball is moved instead of the device. Used mainly for notebooks.

Trademark—A registered word, letter, or device granting the owner exclusive rights to sell or distribute the goods to which it is applied.

Trading partner agreement—A contractual arrangement that specifies the legal terms and conditions under which parties operate when conducting transactions by the use of EDI. It may cover such things as: validity and formation of contract; admissibility in evidence of EDI messages; processing and acknowledgment of receipt of EDI messages; security; confidentiality and protection of personal data; recording and storage of EDI messages; operational requirements for EDI--message standards, codes, transaction and operations logs; technical specifications and requirements; liability, including use of intermediaries and third party service providers; dispute resolution; and, applicable law.

Traditional technology approach—Has two primary views of any system — information and procedures — and it keeps these two views separate and distinct at all times.

Traffic analysis—A type of security threat that occurs when an outside entity is able to monitor and analyze traffic patterns on a network.

Traffic flow confidentiality—A confidentiality service to protect against traffic analysis.

Traffic flow security—The protection that results from those features in some cryptography equipment that conceal the presence of valid messages on a communications circuit, usually by causing the circuit to appear busy at all times or by encrypting the source and destination addresses of valid messages.

Traffic security—a collection of techniques for concealing information about a message to include existence, sender, receivers and duration. Methods of traffic security include call-sign changes, dummy messages and radio silence.

Training—Teaching people the knowledge and skills that will enable them to perform their jobs more effectively.

Training assessment—An evaluation of the training efforts.

Training effectiveness—A measurement of what a given student has learned from a specific course or training event, i.e., learning effectiveness; a pattern of student outcomes following a specific course or training event; teaching effectiveness; and the value of the specific class or training event, compared to other options in the context of an agency's overall IT security training program; program effectiveness.

Training effectiveness evaluation—Information collected to assist employees and their supervisors in assessing individual students' subsequent on-the-job performance, to provide trend data to assist trainers in improving both learning and teaching, and to be used in return-on investment statistics to enable responsible officials to allocate limited resources in a thoughtful, strategic manner among the spectrum of IT security awareness, security literacy, training, and education options for optimal results among the workforce as a whole.

Training matrix—A table that relates role categories relative to IT systems.

Transaction—A transaction is an activity or request to a computer. Purchase orders, changes, additions, and deletions are examples of transactions that are recorded in a business information environment.

Transaction Change Request System—A system established under HIPAA for accepting and tracking change requests for any of the HIPAA mandated transactions standards via a single Web site. See www.hipaa-dsmo.org.

Transaction file—A collection of records containing data generated from the current business activity.

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.

Transactional Processing System (TPS)—The processing of transactions as they occur rather than in batches.

Transceiver—The physical device that connects a host interface to a local area network, such as Ethernet. Ethernet transceivers contain electronics that apply signals to the cable and sense collisions.

Transform domain techniques—Various methods of signal and image processing (Fast Fourier Transform, Discrete Cosine Transform, etc.) used mainly for the purposes of compression.

Transformation analysis—The process of detecting areas of image and sound files that is unlikely to be affected by common transformations and hide information in those places. The goal is to produce a more robust watermark.

Translator—See EDI Translator.

Transmission Control Protocol (TCP)—The major transport protocol in the Internet suite of protocols providing reliable, connection-oriented, full-duplex streams.

Transnational firm—A firm that produces and sells products and services all over the world.

Transport layer—The layer of the ISO Reference Model responsible for managing the delivery of data over a communications network.

Transport Layer Security Protocol—The public version of SSL3, being specified by the IETF.

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.

Treated Conference Room (TCR)—A shielded enclosure that provides acoustic and electromagnetic attenuation protection.

Trojan Horse—A computer program that is apparently or actually useful and contains a trapdoor or unexpected code.

Trojan Horse Software—Software the user does not want that is hidden inside software the user wants.

Trojan Horse Virus—Hides inside other software. Usually an attachment or download.

TRP—Trusted path/channels, trusted path.

True search engine—Uses software agent technologies to search the Internet for key words and then places them into indices.

Trust—Reliance on the ability of a system or process to meet its specifications.

Trusted Computer Security Evaluation Criteria (TCSEC)—A security development standard for system manufacturers and a basis for comparing and evaluating different computer systems. Also known as the *Orange Book*.

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.

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. .

Trusted third party—An entity trusted by other entities with respect to security related services and activities, such as a certification authority.

TSE—In Common Criteria, TOE access, TOE session establishment.

TSF—See *TOE Security Functions.*

TSP —In Common Criteria, TOE Security Policy (TSP): the rules defining the required security behavior of a TOE.

TSS—In Common Criteria, Security Target evaluation, TOE summary specification.

TST—In Common Criteria, Protection of the TSF, TSF self test.

TTL—Time-to-live.

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.

Tunneling—The use of authentication and encryption to set up virtual private networks (VPNs).

Turnkey system—A complete, ready-to-operate system that is purchased from a vendor as opposed to a system developed in-house.

Twisted pair—A type of network physical medium made of copper wires twisted around each other. Example: Ordinary telephone cable.

Twisted-pair wire—A communication medium that consists of pairs of wires that are twisted together and bound into cable.

Two-factor authentication—The use of two independent mechanisms for authentication; for example, requiring a smart cart and a password.

Type accreditation—In some situations, a major application or general support system is intended for installation at multiple locations. The application or system usually consists of a common set of hardware, software, and firmware. Type accreditations are a form of interim accreditation and are used to certify and accredit multiple instances of a major application or general support system for operation at approved locations with the same type of computing environment. .

UART—Universal Asynchronous Receiver/Transmitter.

UAU—User authentication.

UB—In HIPAA, Uniform Bill, as in UB-82 or UB-92.

UB-82—In HIPAA, a uniform institutional claim form developed by the NUBC that was in general use from 1983 to 1993.

UB-92—In HIPAA, a uniform institutional claim form developed by the NUBC that has been in general use since 1993.

UCF—In HIPAA, Uniform Claim Form, as in UCF-1500.

UCTF—See the *Uniform Claim Task Force.*

UDP—User Datagram Protocol. Connectionless transport layer protocol in the TCP/IP stack. UDP is a simple protocol that exchanges datagrams without acknowledgments or guaranteed delivery, requiring that error processing and retransmission be handled by other protocols. UDP is defined in RFC 768.

UHIN—See the Utah Health Information Network.

UID—User identification.

UN/CEFACT—See the United Nations Centre for Facilitation of Procedures and Practices for Administration, Commerce, and Transport.

UN/EDIFACT—See the United Nations Rules for Electronic Data Interchange for Administration, Commerce, and Transport.

Unallocated space—The set of clusters that has been marked as available to store information but has not yet received a file, or still contains some or all of a file marked as deleted.

Unauthorized (malicious or accidental) disclosure, modification, or destruction of information— Unintentional errors and omissions.

Unauthorized disclosure—Exposure of information to individuals not authorized to receive it.

Understanding—Real-world knowledge in context.

UNI—User network interface.

Uniform Claim Task Force (UCTF)—In HIPAA, an organization that developed the initial HCFA-1500 Professional Claim Form. The maintenance responsibilities were later assumed by the NUCC.

Uniform Resource Locator (URL)—The primary means of navigating the web; consists of the means of access, the Web site, the path, and the document name of a Web resource, such as http://www.auerbach-publications.com.

Uninstaller software—Utility software that can be used to remove software that the user no longer wants from the hard disk.

Unit Security Officer—A U.S. citizen employee who is a nonprofessional security officer designated with a specific or homogeneous working unit to assist the office of security in carrying out functions prescribed in these regulations.

Unit testing—The testing of a module for typographic, syntactic, and logical errors and for correct implementation of its design and satisfaction of its requirements.

United Nations Centre for Facilitation of Procedures and Practices for Administration, Commerce, and Transport (UN/CEFACT)—An international organization dedicated to the elimination or simplification of procedural barriers to international commerce.

United Nations Rules for Electronic Data Interchange for Administration, Commerce, and Transport (UN/EDIFACT)—An international EDI format. Interactive X12 transactions use the EDIFACT message syntax.

Universal Product Code (UPC)—An array of varied width lines that can be read by special machines (e.g., OCR devices) and converted into alphanumeric data. This method is used to mark merchandise for direct input of sales transactions.

UNIX—An operating system initially developed by Bell Labs. Used primarily on engineering workstations and computers, and networked systems. UNIX is difficult for nontechnical people to use but is becoming increasingly popular in the business environment in supporting GUI applications.

UNL—Privacy, unlinkability.

UNO—Privacy, unobservability.

Unshielded Twisted Pair (UTP)—A generic term for "telephone" wire used to carry data such as 10Base-T and 100Base-T. Various categories (qualities) of cable exist that are certified for different kinds of networking technologies.

UNSM—United Nations Standard Messages.

Unstructured Data—See Data-Related Concepts.

Update—The file processing activity in which master records are altered to reflect the current business activity contained in transactional files.

Upgrading—The determination that particular unclassified or classified information requires a higher degree of protection against unauthorized disclosure than currently provided. Such determination shall be coupled with a marking of the material with the new designation.

UPIN—Universal Provider Identification Number--to be replaced by National Provider Identifier under HIPAA.

Uplink frequencies—In satellites, the frequency used from the earth station up to the satellite. In data, the frequency used to send data from a station to a head end or mainframe.

UR—In HIPAA, utilization review.

URAC—The American Accreditation HealthCare Commission.

URL (Uniform Resource Locator)—An address for a specific Web page or document within a Web site.

USB—Identification and authentication user–subject binding.

USB (Universal Serial Bus)—It is becoming the most popular means of connecting devices to a computer. Most standard desktops today have at least 2 USB ports, and most standard notebooks have at least one.

USC or U.S.C—United States Code.

Use—With respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information. (See Disclosure, in contrast.).

USENET—A facility of the Internet, also called "the news," that allows users to read and post messages to thousands of discussion groups on various topics.

Usenet—A worldwide collection/system of newsgroups that allows users to post messages to an online bulletin board.

User—(1) The party, or his designee, responsible for the security of designated information. The user works closely with an ISSE. Also referred to as the customer. (2) Person or process accessing an AIS either by direct connections (i.e., via terminals), or indirect connections (i.e., prepare input data or receive output that is not reviewed for content or classification by a responsible individual).

User Acceptance Testing (UAT)—Determines if the system satisfies the business requirements and enables the knowledge workers to perform their jobs correctly.

User agent—An intelligent agent that takes action on the user's behalf.

User Datagram Protocol (UDP)—A transport protocol in the Internet suite of protocols. UDP, like TCP, uses IP for delivery; however, unlike TCP, UDP provides for exchange of datagrams without acknowledgments or guaranteed delivery.

User documentation—Highlights how to use the system.

User information—The individual, or organization, who has been authorized access to the information asset by the owner.

User interface management—The component of the expert system that is used to run a consultation.

User representative—An individual that represents the operational interests of the user community and serves as the liaison for that community throughout the system development life cycle of the information system.

User/subscriber—An individual procuring goods or services online who obtains a certificate from a certification authority. Since both consumers and merchants may have digital certificates which are used to conclude a transaction, they may both be subscribers in certain circumstances. This person may also be referred to as the signer of a digital signature or the sender of data message signed with a digital signature.

User's identification—A character string which validates authorized user access.

USR—Guidance documents, user guidance.

Utah Health Information Network (UHIN)—Under HIPAA, a public-private coalition for reducing healthcare administrative costs through the standardization and electronic exchange of healthcare data.

Utility software—Software that provides additional functionality to the operating system.

UTP—Unshielded twisted pair.

Valid—Logically correct (with respect to original data, software, or system).

Validation—The determination of the correctness, with respect to the user needs and requirements, of the final program or software produced from a development project.

Validation phase—The users, acquisition authority, and DAA agree on the correct implementation of the security requirements and approach for the completed IS.

Validation, verification, and testing—Used as an entity to define a procedure of review, analysis, and testing throughout the software life cycle to discover errors; the process of validation, verification, and testing determines that functions operate as specified and ensures the production of quality software.

Value chain—A tool that views the organization as a chain or series of processes, each of which adds value to the product or service for the customer.

Value network—All the resources behind the click on a Web page that the customer does not see, but that together create the customer relationship-service, order fulfillment, shipping, financing, information brokering, and access to other products.

Value-Added Network (VAN)—A communications network using existing common carrier networks and providing such additional features as message switching and protocol handling.

VBR—Variable bit rate.

VC—Virtual circuit.

VCI—Virtual channel identifier (X.25).

VCN—Virtual circuit number (X.25).

Vector—Also known as "attack vector" routes or methods used to get into computer systems, usually for nefarious purposes. They take advantage of known weak spots to gain entry. Many attack vectors take advantage of the human element in the system because that is often the weakest link.

Vector image—a digital image that is created through a sequence of commands or mathematical statements that places lines and shapes in a given two or three-dimensional space.

Verification—(1) The authentication process by which the biometric system matches a captured biometric against the person's stored template. (2) The demonstration of consistency, completeness, and correctness of the software at and between each stage of the development life cycle.

Verification phase—The process of determining compliance of the evolving IS specification, design, or code with the security requirements and approach agreed on by the users, acquisition authority, and DAA.

Verify—To determine accurately that (a) the digital signature was created by the private key corresponding to the public key and (b) the message has not been altered since its digital signature was created.

Verify a signature—Perform a cryptographic calculation using a message, a signature for the message, and a public key, to determine whether the signature was generated by someone knowing the corresponding private key.

Versatility—Versatility is the ability to adapt readily to unforeseen requirements. The subordinate elements of versatility are flexibility, interoperability, and autonomy.

Vertical market software—Application software that is unique to a particular industry.

Video disk—An optical disk that can store images.

Videotext—Generic text that refers to a computer information system that uses television, telecommunication, and computer technologies to access and manipulate large, graphics-oriented databases.

Virtual circuit—A network service that provides connection-oriented service, regardless of the underlying network structure.

Virtual marketing—Encourages users of a product or service supplied by a B2C (buyer to customer) company to ask friends to join.

Virtual memory—A method of extending computer memory using secondary storage devices to store program pages that are not being executed at the time.

Virtual Private Network (VPN)—A secure private network that uses the public telecommunications infrastructure to transmit data. In contrast to a much more expensive system of owned or leased lines that can only be used by one company, VPNs are used by enterprises for both extranets and wide are intranets. Using encryption and authentication, a VPN encrypts all data that passes between two Internet points, maintaining privacy and security.

Virtual reality—A three-dimensional computer simulation in which the user actively and physically participates.

Virtual workplace—A technology-enabled workplace — no walls, no boundaries, work anytime, anyplace. Linked to other people and information the user needs.

Virus—A type of malicious software that can destroy the computer's hard drive, files, and programs in memory, and that replicates itself to other disks.

Virus signature files—A file of virus patterns that are compared with existing files to determine if they are infected with a virus. The vendor of the antivirus software updates the signatures frequently and makes the available to customers via the web.

Visible noise—The degradation of a cover as a result of embedding information. Visible noise will indicate the existence of hidden information.

Visible watermark—A visible and translucent image that is overlaid on a primary image. Visible watermarks allow the primary image to be viewed, but still marks it clearly as property of the owner. A digitally watermarked document, image, or video clip can be thought of as digitally "stamped". .

VLA—Vulnerability assessment, vulnerability analysis.

VLAN—Virtual local area network.

VLSM—Variable-length subnet mask.

Voice mail—An e-mail system that allows a regular voice message to be digitally stored at the receiving location and converted back to voice form when it is accessed.

Voice processing—A system that recognizes spoken words as well as touch tones from telephones. Basically, a "voice" computer in that it (theoretically) can do anything a computer can do, and can recognize voice commands.

Voice synthesizer—An input and output device that can either interpret and convert human speech into digital signals for computer processing or convert digital signals into audible signals that resemble human speech.

Volt—The unit of measurement of electromotive force. It is expressed as the potential difference in available energy between two points. One volt is the force required to produce a current of one ampere through a resistance or impedance of 1 ohm.

Voltage—The pressure under which a flow of electrons moves through a device.

VPN—Virtual Private Network--A private network that is configured within a public network.

VTAM—Virtual Terminal Access Method.

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.

Vulnerability analysis—The systematic examination of systems in order to determine the adequacy of security measures, identify security deficiencies, and provide data from which to predict the effectiveness of proposed security measures.

Vulnerability assessment—Systematic examination of an IS or product to determine the adequacy of security measures identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

WAIS—Wind Area Information Server.

Walker—An input device that captures and records the movement of the feet as the user walks or turns in different directions.

Walk-through—A manual analysis technique in which the module author or developer describes the module's structure and logic to colleagues.

WAN (Wide Area Network)—Data communications network that serves users across a broad geographic area and often uses transmission devices provided by common carriers. Frame Relay, SMDS, and X.25 are examples of WANs. *Compare with* LAN and MAN.

Warez—Pronounced *wayrz* or *wayrss*. Commercial software that has been pirated and made available to the public via an electronic bulletin board system (BBS) or the Internet. Typically, the pirate has figured out a way to deactivate the copy protection or registration scheme used by the software. Note that the use and distribution of warez software is illegal. In contrast, shareware and freeware may be freely copied and distributed.

Warm site—A warm site is similar to a hot site; however, it is not fully equipped with all necessary hardware needed for recovery.

Washington Publishing Company (WPC)—Under HIPAA, the company that publishes the X12N HIPAA Implementation guides and the X12N HIPAA Data Dictionary, developed the X12 Data Dictionary, and hosts the EHNAC STFCS testing program.

Waterfall life cycle—A software development process that structures the analysis, design, programming, and testing. Each step is completed before the next step begins.

Watermarking—a form of marking that embeds copyright information about the artist or owner.

Watt—The unit of electricity consumption and representing the product of amperage and voltage.

Waveforms—The characteristic shape of a signal usually shown as a plot of amplitude over a period of time.

Waveguide—A conducting or dielectric structure able to support and propagate one or more modes. More specifically, a hollow, finely engineered metallic tube used to transmit microwave radio signals from the microwave antenna to the radio and vice versa.

Wavelength—The length of a wave measured from any point on one wave to the corresponding point on the next wave.

WDM—Wavelength-division multiplexing.

Wearable computer—A fully equipped computer that is worn just like a piece of clothing or attached to a piece of clothing similar to the way the cell phone is carried on the belt.

Web authoring software—Helps design and develop Web sites and pages that are published on the Web.

Web beacon—Web beacons are images that are placed in HTML documents (Web pages, HTML e-mail) to facilitate user activity tracking. Web beacons are usually used in conjunction with cookies and are often used to track visitors across multiple internet domains. Web beacon images are usually, but not always, small and “invisible.” .

Web browser software—Enables the user to surf the Web.

Web bugs—Small image in an HTML page with all dimensions set to 1 pixel. Because of its insignificant size, it is not visible but used to pass certain information anonymously to third-party sites. Mainly used by advertisers. Can also be referred to as a Web beacon or invisible GIF. .

Web crawler—A software program that searches the Web for specified purposes such as to find a list of all URLs within a particular site.

Web defacement—Also referred to as *defacement* or *Web site defacement*, a form of malicious hacking in which a Web site is “vandalized.” Often the malicious hacker will replace the site’s normal content with a specific political or social message or will erase the content from the site entirely, relying on known security vulnerabilities for access to the site's content.

Web farm—Either a Web site that has multiple servers or an ISP that provides Web site outsourcing services using multiple servers.

Web hosting—The business of providing the equipment and services required to host and maintain files for one or more Web sites and to provide fast Internet connections to those sites. Most hosting is "shared," which means that web sites of multiple companies are on the same server in order to share costs.

Web log—Most Web servers produce "log files," time stamped lists of every request that the server receives. For each request, the log file contains anonymous information such as date and time, the IP address of the browser making the request, the document or action that is being requested, the location of the document from which the request was made, and the type of browser that was being used. Log files are usually used to assure quality of service. They also can be used in a limited way to analyze visitor activity. .

Web page—A specific portion of a Web site that deals with a certain topic.

Web portal—A site that provides a wide range of services including search engines, free e-mail, chat rooms, discussion boards, and links to hundreds of different sites.

Web server—Using the client-server model and the World Wide Web's HyperText Transfer Protocol (HTTP), Web Server is a software program that serves web page files to users.

Web services—Software applications that talk to other software applications over the Internet using XML as a key enabling technology.

Web site—A specific location on the Web where the user can visit, gather information, and order products.

Web site address—unique name that identifies a specific site on the Web.

Web space—A storage area where the user's Web site can be kept.

WEDI—Workgroup on Electronic Data Interchange.

WFQ—Weighted Fair Queuing.

WG—Under HIPAA, work group.

Whitehat (or ethical) hacker—A computer security professional who is hired by a company to break into its computer system.

WHO—See the World Health Organization.

Whois—An Internet resource that permits users to initiate queries to a database containing information on users, hosts, networks, and domains.

Wide Area Networks (WAN)—A communications network that covers a broad geographic area.

WiFi (wireless fidelity)—A way of transmitting information in a wave form that is reasonably fast and is often used for notebooks. Also known as IEEE 802.11b.

Wired communications—Media that transmit information over a closed connected path.

Wireless communications—Media that transmit information through the air.

Wireless Internet Service Provider (wireless ISP)—A company that provides the same services as a standard Internet service provider except that the user does not need a wired connection for access.

Wireless Local Area Network (WLAN)—A local area network using wireless communication protocol.

Wireless Local Loop (WLL)—A means of provisioning a local loop facility without wires. Employing low power, omnidirectional radio systems, they allow carriers to provision loops up to T-1 capacity to each subscriber.

Wireless network access point—A device that allows computers to access a network using radio waves.

Wiring closet—Specially designed room used for wiring a data or voice network. Wiring closets serve as a central junction point for the wiring and wiring equipment that is used for interconnecting devices.

Wisdom—Understanding of what is true, right or lasting.

Word—In computer memory, a contiguous set of bits used as a basic unit of storage. Words are usually 8,16, 32, or 64 bits long.

Word processing—The use of computers or other technology for storage, editing, correction, revision, and production of textual files in the form of letters, reports, and documents.

Work factor—The effort and time required to break a protective measure.

Workflow—Defines all of the steps or business rules, from beginning to end, required for a process to run correctly.

Workforce—Under HIPAA, employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity. (See business associate, in contrast.).

Workgroup—A group of people who can work together to achieve a common set of goals, linked together via technological tools and hardware.

Workgroup for Electronic Data Interchange (WEDI)—A healthcare industry group that lobbied for HIPAA A/S, and that has a formal consultative role under the HIPAA legislation. WEDI also sponsors SNIP.

World Health Organization (WHO)—An organization that maintains the International Classification of Diseases (ICD) medical code set.

World Wide Web or Web—A multimedia-based collection of information, services, and Web sites supported by the Internet.

Worm—With respect to security, a special type of virus that does not attach itself to programs, but rather spreads via other methods such as e-mail.

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

WPC— See the Washington Publishing Company.

Wrapper—See *cover medium.*

WWW—World Wide Web; also shortened to Web. Although WWW is used by many as being synonymous to the Internet, the WWW is actually one of numerous services on the Internet. This service allows e-mail, images, sound, and newsgroups.

X.25—WAN Protocol.

X.400—A ITU-TSS international standard for reformatting and sending Internet work via e-mail.

X.500—The CITT and ISO standard for electronic directory services.

X.509—A standard which is part of the X.500 specifications which defines the format of a public key certificate.

X/recommendations—The ITU-TSS documents that describe data communication network standards. Well-known ones include: X.25 Packet Switching Standard, X.400 Message Handling System, and X.500 Directory Services.

X12—An ANSI-accredited group that defines EDI standards for many American industries, including healthcare insurance. Most of the electronic transaction standards mandated or proposed under HIPAA are X12 standards.

X12 Standard—The term currently used for any X12 standard that has been approved since the most recent release of X12 American National Standards. Because a full set of X12 American National Standards is only released about once every five years, it is the X12 standards that are most likely to be in active use. These standards were previously called Draft Standards for Trial Use.

X12/PRB—In HIPAA, The X12 Procedures Review Board.

XDSL—A group term used to refer to ADSL (Asymmetrical Digital Subscriber Line), HDSL (High data rate Digital Subscriber Line), and SDSL (Symmetrical Digital Subscriber Line). All are digital technologies using the existing copper infrastructure provided by the telephone companies. XDSL is a high-speed alternative to ISDN.

XML (eXtensible Markup Language)—A coding language for the Web that lets computers interpret the meaning of information in Web documents.

XNS—Xerox Network Systems.

X-Open—A group of computer manufacturers who promote the development of portable applications based on UNIX. They publish a document called the X-Open Portability Guide.

XOR—The XOR (exclusive-OR) gate acts in the same way as the logical "either/or." The output is "true" if either, but not both, of the inputs are "true." The output is "false" if both inputs are "false" or if both inputs are "true." Another way of looking at this circuit is to observe that the output is 1 if the inputs are different, but 0 if the inputs are the same.

XOT—X.25 over TCP.

YCbCr—A setting used in the representation of digital images. Y is the luminance component; Cb,Cr are the chrominance components.

Zero Code Suppression (ZCS)—The insertion of a "1" bit to prevent the transmission of eight or more consecutive "0" bits.

ZIP—Zone Information Protocol (AppleTalk).

Zip drive—A high capacity, removeable diskette drive that typically uses 100MB Zip disks or cartridges.

ZIT—Zone Information Table (AppleTalk).