Appendix eL

# Glossary

**AAA** Administration, authorization, and authentication.

**Access** A specific type of interaction between a subject and an object that results in the flow of information from one to the other. The capability and opportunity to gain knowledge of, or to alter information or materials including the ability and means to communicate with (i.e., input or receive output), or otherwise make use of any information, resource, or component in a computer system.

**Access Control** The process of limiting access to the resources of a system to only authorized persons, programs, processes, or other systems. Synonymous with controlled access and limited access. Requires that access to information resources be controlled by or for the target system. In the context of network security, access control is the ability to limit and control the access to host systems and applications via communications links. To achieve this control, each entity trying to gain access must first be identified, or authenticated, so that access rights can be tailored to the individual.

**Accreditation** The written formal management decision to approve and authorize an organization to operate a classified information system (IS) to process, store, transfer, or provide access to classified information.

**Accreditation/Approval** The official management authorization for operation of an MIS. It provides a formal declaration by an Accrediting Authority that a computer system is approved to operate in a particular security mode using a prescribed set of safeguards. Accreditation is based on the certification process as well as other management considerations. An accreditation statement affixes security responsibility with the Accrediting Authority and shows that proper care has been taken for security.

**Activities** An assessment object that includes specific protectionrelated pursuits or actions supporting an information system that involve people (conducting system backup operations, monitoring network traffic).

**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 used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost-effective management, personnel, operational and technical controls.

**ADP** Automatic Data Processing. See also: Management Information System.

**AES** Advanced Encryption Standard.

**Agency** See: *Executive Agency*.

**Agent** A host-based intrusion detection and prevention program that monitors and analyzes activity and may also perform prevention actions.

**Alert** A notification of an important observed event.

**Anomaly-Based Detection** The process of comparing definitions of what activity is considered normal against observed events to identify significant deviations.

**Antivirus Software** A program that monitors a computer or network to identify all major types of malware and prevent or contain malware incidents.

**Application** A software organization of related functions, or series of interdependent or closely related programs, that when executed accomplish a specified objective or set of user requirements. See also: Major Application, Process.

**Application-Based Intrusion Detection and Prevention System** A host-based intrusion detection and prevention system that performs monitoring for a specific application service only, such as a Web server program or a database server program.

**Application Control** The ability for next generation content filter gateways to inspect the application and determine its intention and block accordingly.

**Application Layer** The seventh layer of the Open Systems Interconnection (OSI) model. The point where the user application interfaces with the protocols to transfer data across the network.

**Application Owner** The official who has the responsibility to ensure that the program or programs, which make up the application accomplish the specified objective or set of user requirements established for that application, including appropriate security safeguards. See also: Process Owner.

**Assessment** See: *Security Control Assessment*.

**Assessment Findings** Assessment results produced by the application of an assessment procedure to a security control or control enhancement to achieve an assessment objective; the execution of a determination statement within an assessment procedure by an assessor that results in either a *satisfied* or *other than satisfied* condition.

**Assessment Method** One of three types of actions (examine, interview, test) taken by assessors in obtaining evidence during an assessment.

**Assessment Object** The item (specifications, mechanisms, activities, individuals) upon which an assessment method is applied during an assessment.

**Assessment Objective** A set of determination statements that expresses the desired outcome for the assessment of a security control or control enhancement.

**Assessment Procedure** A set of assessment *objectives* and an associated set of assessment *methods* and assessment *objects*.

**Assessor** See: *Security Control Assessor*.

**Assurance** The grounds for confidence that the set of intended security controls in an information system are effective in their application.

**Assurance Case** A structured set of arguments and a body of evidence showing that an information system satisfies specific claims with respect to a given quality attribute.

**Attachment** The blocking of certain types of file (executable programs).

**Audit** To conduct the independent review and examination of system records and activities.

**Audit Capability** The ability to recognize, record, store, and analyze information related to security-relevant activities on a system in such a way that the resulting records can be used to determine which activities occurred and which user was responsible for them.

**Audit Trail** A set of records that collectively provides documentary evidence of processing. It is used to aid in tracing from original transactions forward to related records and reports, and/or backwards from records and reports to their component source transactions.

**Automated Information Systems (AIS)** The infrastructure, organization, personnel, and components for the collection, processing, storage, transmission, display, dissemination, and disposition of information.

**Automatic Data Processing (ADP)** The assembly of computer hardware, firmware, and software used to categorize, sort, calculate, compute, summarize, store, retrieve, control, process, and/or protect data with a minimum of human intervention. ADP systems can include, but are not limited to, process control computers, embedded computer systems that perform general purpose computing functions, supercomputers, personal computers, intelligent terminals, offices automation systems (which includes standalone microprocessors, memory typewriters, and terminal connected to mainframes), firmware, and other implementations of MIS technologies as may be developed: they also include applications and operating system software. See also: Management Information System.

**Authenticate/Authentication** The process to verify the identity of a user, device, or other entity in a computer system, often as a prerequisite to allowing access to resources in a system. Also, a process used to verify that the origin of transmitted data is correctly identified, with assurance that the identity is not false. To establish the validity of a claimed identity.

**Authenticated User** A user who has accessed a MIS with a valid identifier and authentication combination.

**Authenticator** A method of authenticating a classified information system (IS) in the form of knowledge or possession (for example, password, token card, key).

**Authenticity** The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. See: Authentication.

**Authorization** The privileges and permissions granted to an individual by a designated official to access or use a program, process, information, or system. These privileges are based on the individual's approval and need-to-know.

**Authorization Boundary** All components of an information system to be authorized for operation by an authorizing official and excludes separately authorized systems, to which the information system is connected.

**Authorizing Official** A senior (federal) official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.

**Authorized Person** A person who has the need-to-know for sensitive information in the performance of official duties and who has been granted authorized access at the required level. The responsibility for determining whether a prospective recipient is an authorized person rests with the person who has possession, knowledge, or control of the sensitive information involved, and not with the prospective recipient.

**Authorizing Official Designated Representative** An organizational official acting on behalf of an authorizing official in carrying out and coordinating the required activities associated with security authorization.

**Availability** The property of being accessible and usable upon demand by an authorized entity. Security constraints must make MIS services available to authorized users and unavailable to unauthorized users.

**Availability of Data** The state when data are in the place needed by the user, at the time the user needs them, and in the form needed by the user.

**Backdoor** A malicious program that listens for commands on a certain Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) port.

**Backup** A copy of a program or data file for the purposes of protecting against loss if the original data becomes unavailable.

**Backup and Restoration of Data** The regular copying of data to separate media and the recovery from a loss of information.

**Backup Operation** A method of operations to complete essential tasks as identified by a risk analysis. These tasks would be employed following a disruption of the MIS and continue until the MIS is acceptably restored. See also: Contingency Plan, Disaster Recovery.

**Bad Reputation Domains** Sites that appear on one or more security industry blacklists for repeated bad behavior, including hosting malware and phishing sites, generating spam, or hosting content linked to by spam email.

**Bandwidth** A measure of spectrum (frequency) use or capacity. For instance, a voice transmission by telephone requires a

bandwidth of about 3000 cycles per second (3 KHz). A television channel occupies a bandwidth of 6 million cycles per second (6 MHz) in terrestrial Systems. In satellite-based systems a larger bandwidth of 17.5 to 72 MHz is used to spread or "dither" the television signal in order to prevent interference.

**Basic Testing** A test methodology that assumes no knowledge of the internal structure and implementation detail of the assessment object. Also known as black box testing.

**Bent Pipe** A description of a satellite communication architecture type in which data is transmitted to the satellite, which then sends it right back down again like a bent pipe. The only processing performed is retransmission of the signals.

**Black Box Testing** See: *Basic Testing*.

**Blacklist** A list of discrete entities, such as hosts or applications, that have been previously determined to be associated with malicious activity.

**Blended Attack** An instance of malware that uses multiple infection or transmission methods.

**Blinding** Generating network traffic that is likely to trigger many alerts in a short period of time, to conceal alerts triggered by a "real" attack performed simultaneously.

**Boot Sector Virus** A virus that infects the master boot record (MBR) of a hard drive or the boot sector of removable media, such as floppy diskettes.

**Botnet** Sites used by botnet herders for command and control of infected machines. Sites that known malware and spyware connects to for command and control by cyber criminals. These sites are differentiated from the Malcode category to enable reporting on potentially infected computers inside the network.

**By URL** Filtering based on the URL. This is a suitable for blocking Web sites or sections of Web sites.

**C2** A level of security safeguard criteria. See also: Controlled Access Protection, TCSEC.

**Capstone** The U.S. Government's long-term project to develop a set of standards for publicly-available cryptography, as authorized by the Computer Security Act of 1987. The Capstone cryptographic system will consist of four major components and be contained on a single integrated circuit microchip that provides nonDoD data encryption for Sensitive But Unclassified information. It implements the Skipjack algorithm. See also: Clipper.

**Certification** The comprehensive analysis of the technical and nontechnical features, and other safeguards, to establish the extent to which a particular MIS meets a set of specified security requirements. Certification is part of the accreditation process and carries with it an implicit mandate for accreditation. See also: Accreditation.

**Channel** An information transfer path within a system or the mechanism by which the path is affected.

**Channel Scanning** Changing the channel being monitored by a wireless intrusion detection and prevention system.

**CHAP** Challenge Handshake Authentication Protocol developed by the IETF.

**Chief Information Officer** Agency official responsible for: (i) Providing advice and other assistance to the head of the executive agency and other senior management personnel of the agency to ensure that information technology is acquired and information resources are managed in a manner that is consistent with laws, Executive Orders, directives, policies, regulations, and priorities established by the head of the agency; (ii) Developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture for the agency; and (iii) Promoting the effective and efficient design and operation of all major information resources management processes for the agency, including improvements to work processes of the agency.

**Chief Information Security Officer** See: *Senior Agency Information Security Officer.*

**Child Pornography** Sites that promote, discuss or portray children in sexual acts and activity or the abuse of children. Pornographic sites that advertise or imply the depiction of underage models and that do not have a U.S.C. 2257 declaration on their main page. As of March 13, 2007, all sites categorized as child porn are actually saved into the URL Library in the Porn category and are automatically submitted to the Internet Watch Foundation for legal verification as child pornography (http://www.iwf.org.uk/). If the IWF agrees that a site and/or any of its hosted pages are child pornography, they add it those URLs to their master list. The master list is downloaded nightly and saved into the URL Library in the Child Porn category.

**Cipher** An algorithm for encryption or decryption. A cipher replaces a piece of information (an element of plain text) with another object, with the intent to conceal meaning. Typically, the replacement rule is governed by a secret key. See also: Decryption, Encryption.

**Ciphertext** Form of cryptography in which the *plaintext* is made unintelligible to anyone who intercepts it by a transformation of the information itself, based on some key.

**CIO-Cyber Web Site** Provides training modules for Cyber Security subjects.

**Classification** A systematic arrangement of information in groups or categories according to established criteria. In the interest of national security it is determined that the information requires a specific degree of protection against unauthorized disclosure together with a designation signifying that such a determination has been made.

**Classified Distributive Information Network (CDIN)** Any cable, wire, or other approved transmission media used for the clear text transmission of classified information in certain DOE access controlled environments. Excluded is any system used solely for the clear text transmission and reception of intrusion/fire alarm or control signaling.

**Classified Information System (CIS)** A discrete set of information resources organized for the collection, processing, maintenance, transmission, and dissemination of classified information, in accordance with defined procedures, whether automated or manual. Guidance Note: For the purposes of this document, an IS may be a standalone, single- or multi-user system or a network comprised of multiple systems and ancillary supporting communications devices, cabling, and equipment.

**Classified Information Systems Security Plan (ISSP)** The basic classified system protection document and evidence

that the proposed system, or update to an existing system, meets the specified protection requirements. The Classified ISSP describes the classified IS, any interconnections, and the security protections and countermeasures. This plan is used throughout the certification, approval, and accreditation process and serves for the lifetime of the classified system as the formal record of the system and its environment as approved for operation. It also serves as the basis for inspections of the system.

**Classified Information Systems Security Program** The Classified Information Systems Security Program provides for the protection of classified information on information systems at LANL.

**Classified Information Systems Security Site Manager (ISSM)** The manager responsible for the LANL Classified Information Systems Security Program.

**Clear or Clearing (MIS Storage Media)** The removal of sensitive data from MIS storage and other peripheral devices with storage capacity, at the end of a period of processing. It includes data removal in such a way that assures, proportional to data sensitivity, it may not be reconstructed using normal system capabilities, i.e., through the keyboard. See also: Object Reuse, Remanence.

**Clipper** Clipper is an encryption chip developed and sponsored by the U.S. government as part of the Capstone project. Announced by the White House in April 1993, Clipper was designed to balance competing concerns of federal law-enforcement agencies and private citizens by using escrowed encryption keys. See also: Capstone, Skipjack.

**Collaborator** A person not employed by the Laboratory who (1) is authorized to remotely access a LANL unclassified computer system located on the site or (2) uses a LANL system located off the site. Guidance note: A collaborator does not have an active Employee Information System record.

**Commercial-off-the-Shelf (COTS)** Products that are commercially available and can be utilized as generally marketed by the manufacturer.

**Common Control** A security control that is inherited by one or more organizational information systems. See: *Security ControlInheritance*.

**Common Control Provider** An organizational official responsible for the development, implementation, assessment, and monitoring of common controls (security controls inherited by information systems).

**Communications Ground Station** Telecommunications network nodes communicate through satellites, typically with small antennas and low-cost electronics at user facilities, and large antennas with more complex data handling facilities at key traffic hubs. Hub Earth stations are generally owned by satellite operators or specialized satellite network providers.

**Communications Security (COMSEC)** Measures and controls taken to deny unauthorized individuals information derived from telecommunications and to ensure the authenticity of such telecommunications. Communications security includes cryptosecurity, transmission security, emission security, and physical security of COMSEC material.

**Compensating Security Controls** The management, operational, and technical controls (safeguards or countermeasures) employed by an organization in lieu of the recommended controls in the baselines described in NIST Special Publication 800-53 and CNSS Instruction 1253, that provide equivalent or comparable protection for an information system.

**Compiled Viruses** A virus that has had its source code converted by a compiler program into a format that can be directly executed by an operating system.

**Comprehensive Testing** A test methodology that assumes explicit and substantial knowledge of the internal structure and implementation detail of the assessment object. Also known as white box testing.

**Compromise** The disclosure of sensitive information to persons not authorized access or having a need-to-know.

**Computer Fraud and Abuse Act of 1986** This law makes it a crime to knowingly gain access to a federal government computer without authorization and to affect its operation.

**Computer Security** Technological and managerial procedures applied to MIS to ensure the availability, integrity, and confidentiality of information managed by the MIS. See also: Information Systems Security.

**Computer Security Act of 1987** The law provides for improving the security and privacy of sensitive information in "federal computer systems"—"a computer system operated by a federal agency or other organization that processes information (using a computer system) on behalf of the federal government to accomplish a federal function."

**Computer Security Incident** Any event or condition having actual or potentially adverse effects on an information system. See the Cyber Security Handbook.

**Computing, Communications, and Networking (CCN) Division Web Sites** Describes network services and their use by system users.

**Confidentiality** The condition when designated information collected for approved purposes is not disseminated beyond a community of authorized knowers. It is distinguished from secrecy, which results from the intentional concealment or withholding of information. [OTA-TCT-606] Confidentiality refers to: 1) how data will be maintained and used by the organization that collected it; 2) what further uses will be made of it; and 3) when individuals will be required to consent to such uses. It includes the protection of data from passive attacks and requires that the information (in an MIS or transmitted) be accessible only for reading by authorized parties. Access can include printing, displaying, and other forms of disclosure, including simply revealing the existence of an object.

**Configuration Management (CM)** The management of changes made to an MIS hardware, software, firmware, documentation, tests, test fixtures, test documentation, communications interfaces, operating procedures, installation structures, and all changes there to throughout the development and operational life-cycle of the MIS.

**Console** A program that provides user and administrator interfaces to an intrusion detection and prevention system.

**Contingency Plan** The documented organized process for implementing emergency response, backup operations, and post-disaster recovery, maintained for an MIS as part of its

security program, to ensure the availability of critical assets (resources) and facilitate the continuity of operations in an emergency. See also: Disaster Recovery.

**Contingency Planning** The process of preparing a documented organized approach for emergency response, backup operations, and post-disaster recovery that will ensure the availability of critical MIS resources and facilitate the continuity of MIS operations in an emergency. See also: Contingency Plan, Disaster Recovery.

**Control Segment** Responsible for the operation of the overall satellite system, which includes platform control, payload control, and network control. The control segment consists of ground satellite control facilities, systems onboard the satellite and communications networks linking the control facilities.

**Controlled Access Protection (C2)** A category of safeguard criteria as defined in the Trusted Computer Security Evaluation Criteria (TCSEC). It includes identification and authentication, accountability, auditing, object reuse, and specific access restrictions to data. This is the minimum level of control for SBU information.

**Controlled Unclassified Information** A categorical designation that refers to unclassified information that does not meet the standards for National Security Classification under Executive Order 12958, as amended, but is (i) pertinent to the national interests of the United States or to the important interests of entities outside the federal government, and (ii) under law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination. Henceforth, the designation CUI replaces *Sensitive But Unclassified (SBU).*

**Conventional Encryption** A form of cryptosystem in which encryption and decryption are performed using the same key. See also: Symmetric Encryption.

**Cookie** A small data file that holds information regarding the use of a particular Web site.

**COTS** See: Commercial-off-the-Shelf.

**COTS Software** Commercial-off the Shelf Software – software acquired by government contract through a commercial vendor. This software is a standard product, not developed by a vendor for a particular government project.

**Countermeasures** See: Security Safeguards.

**Coverage** An attribute associated with an assessment method that addresses the scope or breadth of the assessment objects included in the assessment (types of objects to be assessed and the number of objects to be assessed by type). The values for the coverage attribute, hierarchically from less coverage to more coverage, are basic, focused, and comprehensive.

**Cracker** See: Hacker.

**Criminal Skills** Sites that promote crime or illegal activity such as credit card number generation, illegal surveillance and murder. Sites which commercially sell surveillance equipment will not be saved. Sample sites: www.illegal-world.com, www.password-crackers.com, and www.spy-cam-surveillance-equipment.com

**Critical Assets** Those assets, which provide direct support to the organization's ability to sustain its mission. Assets are critical if their absence or unavailability would significantly degrade the ability of the organization to carry out its mission, and when the time that the organization can function without the asset is less than the time needed to replace the asset.

**Critical Processing** Any applications, which are so important to an organization, that little or no loss of availability is acceptable; critical processing must be defined carefully during disaster and contingency planning. See also: Critical Assets.

**Cryptanalysis** The branch of cryptology dealing with the breaking of a cipher to recover information, or forging encrypted information what will be accepted as authentic.

**Cryptography** The branch of cryptology dealing with the design of algorithms for encryption and decryption, intended to ensure the secrecy and/or authenticity of messages.

**Cryptology** The study of secure communications, which encompasses both cryptography and cryptanalysis.

**Cybersecurity** No formal, accepted definition of cybersecurity currently exists; however, the International Telecommunication Union recently approved ITU-T X.1205 "Overview of Cybersecurity." This document states "cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following: availability, integrity, which may include authenticity and non-repudiation, and confidentiality."

**Cyber Security Program** The program mandated to ensure that the confidentiality, integrity, and availability of electronic data, networks and computer systems are maintained to include protecting data, networks and computing systems from unauthorized access, alteration, modification, disclosure, destruction, transmission, denial of service, subversion of security measures, and improper use.

**Cyberspace** *National Security Presidential Directive 54/ Homeland Security Presidential Directive 23* defines cyberspace as the interdependent network of information technology infrastructures, and include the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries. Common usage of the term also refers to the virtual environment of information and interactions between people.

**DAC** See: C2, Discretionary Access Control and TCSEC.

**DASD (Direct Access Storage Device)** A physical electromagnetic data storage unit used in larger computers. Usually these consist of cylindrical stacked multiunit assemblies, which have large capacity storage capabilities.

**Data** A representation of facts, concepts, information, or instructions suitable for communication, interpretation, or

processing. It is used as a plural noun meaning "facts or information" as in: *These data are described fully in the appendix,* or as a singular mass noun meaning "information" as in: *The data is entered into the computer.*

**Database Server** A repository for event information recorded by sensors, agents, or management servers.

**Data Custodian** The person who ensures that information is reviewed to determine if it is classified or sensitive unclassified. This person is responsible for generation, handling and protection, management, and destruction of the information. Guidance Note: An alternative name for the data custodian is classified information systems application owner.

**Data Encryption Standard (DES)** Data Encryption Standard is an encryption block cipher defined and endorsed by the U.S. government in 1977 as an official standard (FIPS PUB 59). Developed by IBM®, it has been extensively studied for over 15 years and is the most well known and widely used cryptosystem in the world. See also: Capstone, Clipper, RSA, Skipjack.

**Data Integrity** The state that exists when computerized data are the same as those that are in the source documents and have not been exposed to accidental or malicious alterations or destruction. It requires that the MIS assets and transmitted information be capable of modification only by authorized parties. Modification includes writing, changing, changing status, deleting, creating, and the delaying or replaying of transmitted messages. See also: Integrity, System Integrity.

**Deciphering** The translation of encrypted text or data (called ciphertext) into original text or data (called plaintext). See also: Decryption.

**Decryption** The translation of encrypted text or data (called ciphertext) into original text or data (called plaintext). See also: Deciphering.

**Dedicated Security Mode** An operational method when each user with direct or indirect individual access to a computer system, its peripherals, and remote terminals or hosts has a valid personnel security authorization and a valid need-to-know for all information contained within the system.

**Dedicated System** A system that is specifically and exclusively dedicated to and controlled for a specific mission, either for full time operation or a specified period of time. See also: Dedicated Security Mode.

**Default** A value or setting that a device or program automatically selects if you do not specify a substitute.

**Degaussing Media** Method to magnetically erase data from magnetic tape.

**Denial of Service** The prevention of authorized access to resources or the delaying of time-critical operations. Refers to the inability of a MIS system or any essential part to perform its designated mission, either by loss of, or degradation of operational capability.

**Deny by Default** A configuration for a firewall or router that denies all incoming and outgoing traffic that is not expressly permitted, such as unnecessary services that could be used to spread malware.

**Department of Defense (DOD) Trusted Computer System Evaluation Criteria** The National Computer Security Center (NCSC) criteria intended for use in the design and evaluation of systems that will process and/or store sensitive (or classified) data. This document contains a uniform set of basic requirements and evaluation classes used for assessing the degrees of assurance in the effectiveness of hardware and software security controls built in the design and evaluation of MIS. See also: C2, Orange Book, TCSEC.

**Depth** An attribute associated with an assessment method that addresses the rigor and level of detail associated with the application of the method. The values for the depth attribute, hierarchically from less depth to more depth, are basic, focused, and comprehensive.

**DES** See: Data Encryption Standard. See also: Capstone, Clipper, RSA, Skipjack.

**Designated Accrediting Authority (DAA)** A DOE official with the authority to formally grant approval for operating a classified information system; the person who determines the acceptability of the residual risk in a system that is prepared to process classified information and either accredits or denies operation of the system.

**Designated Security Officer** The person responsible to the designated high level manager for ensuring that security is provided for and implemented throughout the life-cycle of an MIS from the beginning of the system concept development phase through its design, development, operations, maintenance, and disposal.

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

**Digital Signature Standard** DSS is the Digital Signature Standard, which specifies a Digital Signature Algorithm (DSA), and is part of the U.S. government's Capstone project. It was selected by NIST and NSA to be the digital authentication standard of the U.S. government, but has not yet been officially adopted. See also: Capstone, Clipper, RSA, Skipjack.

**Disaster Recovery Plan** The procedures to be followed should a disaster (fire, flood, etc.) occur. Disaster recovery plans may cover the computer center and other aspects of normal organizational functioning. See also: Contingency Plan.

**Discretionary Access Control (DAC)** A means of restricting access to objects based on the identity of subjects and/or groups to which they belong or on the possession of an authorization granting access to those objects. The controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (perhaps indirectly) onto any other subject.

**Discretionary access controls** Controls that limit access to information on a system on an individual basis.

**Discretionary processing** Any computer work that can withstand interruption resulting from some disaster.

**Disinfecting** Removing malware from within a file.

**Downlink** The portion of a communications link used to transmit signals from a satellite to an Earth-based terminal (on land, ship, or aircraft).

**DSS** See: Capstone, Clipper, Digital Signature Standard, RSA, Skipjack.

**Dubious/Unsavory** Sites of a questionable legal or ethical nature. Sites which promote or distribute products,

information, or devices whose use may be deemed unethical or, in some cases, illegal: Warez, Unlicensed mp3 downloads, Radar detectors, and Street racing. Sample sites: www.thepayback.com and www.strangereports.com.

**Egress Filtering** Blocking outgoing packets that should not exit a network.

**Emergency Response** A response to emergencies such as fire, flood, civil commotion, natural disasters, bomb threats, etc., in order to protect lives, limit the damage to property and the impact on MIS operations.

**Enciphering** The conversion of plaintext or data into unintelligible form by means of a reversible translation that is based on a translation table or algorithm. See also: Encryption.

**Encryption** The conversion of plaintext or data into unintelligible form by means of a reversible translation that is based on a translation table or algorithm. See also: Enciphering.

**End-to-End** The inclusion of all requisite components necessary to deliver stated information exchange capability from the information producer's information appliance to the intended user information appliance(s). For SATCOM systems, this implies all components from the user access and display devices, sensors, all associated applications to include the various levels of networking and processing, and all related communications transport mechanisms and associated management services.

**Entity** Something that exists as independent, distinct or self-contained. For programs, it may be anything that can be described using data, such as an employee, product, or invoice. Data associated with an entity are called attributes. A product's price, weight, quantities in stock, and description all constitute attributes. It is often used in describing distinct business organizations or government agencies.

**Environment** The aggregate of external circumstance, conditions, and events that affect the development, operation, and maintenance of a system. Environment is often used with qualifiers such as computing environment, application environment, or threat environment, which limit the scope being considered.

**Environment of Operation** The physical surroundings in which an information system processes, stores, and transmits information.

**Evaluation** Evaluation is the assessment for conformance with a preestablished metric, criteria, or standard.

**Evasion** Modifying the format or timing of malicious activity so that its appearance changes but its effect on the target is the same.

**Examine** A type of assessment method that is characterized by the process of checking, inspecting, reviewing, observing, studying, or analyzing one or more assessment objects to facilitate understanding, achieve clarification, or obtain evidence, the results of which are used to support the determination of security control effectiveness over time.

**Executive Agency** An executive department specified in 5 U.S.C., Sec. 101; a military department specified in 5 U.S. C., Sec. 102; an independent establishment as defined in 5 U.S.C., Sec. 104(1); and a wholly owned Government corporation fully subject to the provisions of 31 U.S.C., Chapter 91.

**Facsimile** A document that has been sent, or is about to be sent, via a fax machine.

**False Negative** An instance in which a security tool intended to detect a particular threat fails to do so.

**False Positive** An instance in which a security tool incorrectly classifies benign content as malicious.

**Federal Agency** See: *Executive Agency*.

**Federal Information System** An information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.

**File Infector Virus** A virus that attaches itself to executable programs, such as word processors, spreadsheet applications, and computer games.

**Firewall** A collection of components or a system that is placed between two networks and possesses the following properties: 1) all traffic from inside to outside, and vice-versa, must pass through it; 2) only authorized traffic, as defined by the local security policy, is allowed to pass through it; 3) the system itself is immune to penetration.

**Firmware** Equipment or devices within which computer programming instructions necessary to the performance of the device's discrete functions are electrically embedded in such a manner that they cannot be electrically altered during normal device operations.

**Flooding** Sending large numbers of messages to a host or network at a high rate. In this publication, it specifically refers to wireless access points.

**Flow** A particular network communication session occurring between hosts.

**Focused Testing** A test methodology that assumes some knowledge of the internal structure and implementation detail of the assessment object. Also known as gray box testing.

**Friendly Termination** The removal of an employee from the organization when there is no reason to believe that the termination is other than mutually acceptable.

**Gateway** A machine or set of machines that provides relay services between two networks.

**General Support System** An interconnected set of information resources under the same direct management control which shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people. A system can be, for example, a local area network (LAN) including smart terminals that support a branch office, an agency-wide backbone, a communications network, a departmental data processing center including its operating system and utilities, a tactical radio network, or a shared information processing service organization (IPSO).

**Generic Remote Access** Web sites pertaining to the use of, or download of remote access clients.

**Global SATCOM Support Center** A DoD organization that provides support to joint forces with global operational SATCOM management, maintains situational awareness for current and future SATCOM operations, provides support to anomaly management and resolution, and acts as an interface with the DoD information operations infrastructure.

**Gray Box Testing** See: *Focused Testing*.

**Green Network** See: Open Network.

**Hack** Any software in which a significant portion of the code was originally another program. Many hacked programs simply have the copyright notice removed. Some hacks are done by programmers using code they have previously written that serves as a boilerplate for a set of operations needed in the program they are currently working on. In other cases it simply means a draft. Commonly misused to imply theft of software. See also: Hacker.

**Hacker** Common nickname for an unauthorized person who breaks into or attempts to break into an MIS by circumventing software security safeguards. Also, commonly called a "cracker." See also: Hack, Intruder.

**Hacking** Sites discussing and/or promoting unlawful or questionable tools or information revealing the ability to gain access to software or hardware/communications equipment and/or passwords: Password generation, Compiled binaries, Hacking tools and Software piracy (game cracking). Sample sites: www.happyhacker.org, and www.phreak.com.

**Hardware** Refers to objects that you can actually touch, like disks, disk drives, display screens, keyboards, printers, boards, and chips.

**Heuristic** Filtering based on heuristic scoring of the content based on multiple criteria.

**Hop** A communications signal that travels from the ground to the satellite and back to the ground. In some instances the signal needs to be sent to a second satellite, and then back down to the ground; this is called a double hop or two-hop operation.

**Host-Based Intrusion Prevention System** A program that monitors the characteristics of a single host and the events occurring within the host to identify and stop suspicious activity.

**Hostmaster Database** A relational database maintained by the Network Engineering Group (CCN-5) that contains information about every device connected to the Laboratory unclassified yellow and green networks.

**HTML Anomalies** Legitimate companies keep their Web sites up to date and standards based to support the newest browser version support and features and are malicious code free. Malicious sites frequently have HTML code that is not compliant to standards.

**Hybrid Security Control** A security control that is implemented in an information system in part as a common control and in part as a system-specific control. See: *Common Control* and *System-Specific SecurityControl*.

**Identification** The process that enables recognition of an entity by a system, generally by the use of unique machine-readable usernames.

**IKE** Internet Key Exchange.

**Incident** A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.

**Indication** A sign that a malware incident may have occurred or may be occurring.

**Individuals** An assessment object that includes people applying specifications, mechanisms, or activities.

**Industrial Control System** An information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition systems used to control geographically dispersed assets, as well as distributed control systems and smaller control systems using programmable logic controllers to control localized processes.

**Information** An instance of an information type.

**Information Owner** Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.

**Information Resources** Information and related resources, such as personnel, equipment, funds, and information technology.

**Information Security** 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 Security Officer (ISO)** The person responsible to the designated high level manager for ensuring that security is provided for and implemented throughout the life-cycle of an MIS from the beginning of the system concept development phase through its design, development, operations, maintenance, and disposal.

**Information Security Program Plan** Formal document that provides an overview of the security requirements for an organization-wide information security program and describes the program management controls and common controls in place or planned for meeting those requirements.

**Information System (IS)** The entire infrastructure, organizations, personnel and components for the collection, processing, storage, transmission, display, dissemination and disposition of information.

**Information System Boundary** See: *Authorization Boundary*.

**Information System Owner** (or Program Manager) Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.

**Information Systems Security (INFOSEC)** The protection of information assets from 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. INFOSEC reflects the concept of the totality of MIS security. See also: Computer Security.

**Information System Security Officer (ISSO)** The worker responsible for ensuring that protection measures are installed and operational security is maintained for one or more specific classified information systems and/or networks.

**Information System-related Security Risks** Information system-related security risks are those risks that arise through the loss of confidentiality, integrity, or availability of information or information systems and consider impacts to the organization (including assets, mission, functions,

image, or reputation), individuals, other organizations, and the Nation. See: *Risk*.

**Information Technology** Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.

**Information Type** A specific category of information (privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization or in some instances, by a specific law, Executive Order, directive, policy, or regulation.

**Ingress Filtering** Blocking incoming packets that should not enter a network.

**Inline Sensor** A sensor deployed so that the network traffic it is monitoring must pass through it.

**Integrated Computing Network (ICN)** LANL's primary institutional network.

**Integrity** A subgoal of computer security which ensures that: 1) data is a proper representation of information; 2) data retains its original level of accuracy; 3) data remains in a sound, unimpaired, or perfect condition; 3) the MIS perform correct processing operations; and 4) the computerized data faithfully represent those in the source documents and have not been exposed to accidental or malicious alteration or destruction. See alsoData Integrity, System Integrity.

**Interconnected System** An approach in which the network is treated as an interconnection of separately created, managed, and accredited MIS.

**Internet** A global network connecting millions of computers. As of 1999, the Internet has more than 200 million users worldwide, and that number is growing rapidly.

**Interpreted Virus** A virus that is composed of source code that can be executed only by a particular application or service.

**Interview** A type of assessment method that is characterized by the process of conducting discussions with individuals or groups within an organization to facilitate understanding, achieve clarification, or lead to the location of evidence, the results of which are used to support the determination of security control effectiveness over time.

**Intranet** A network based on TCP/IP protocols (an Internet) belonging to an organization, usually a corporation, accessible only by the organization's members, employees, or others with authorization. An intranet's Web sites look and act just like any other Web sites, but the firewall surrounding an intranet fends off unauthorized access.

**Intruder** An individual who gains, or attempts to gain, unauthorized access to a computer system or to gain unauthorized privileges on that system. See also: Hacker.

**Intrusion Detection** Pertaining to techniques, which attempt to detect intrusion into a computer or network by observation of actions, security logs, or audit data. Detection of breakins or attempts either manually or via software expert systems that operate on logs or other information available on the network.

**Intrusion Detection and Prevention** The process of monitoring the events occurring in a computer system or network, analyzing them for signs of possible incidents, and attempting to stop detected possible incidents. See also "intrusion prevention".

**Intrusion Detection System Load Balancer** A device that aggregates and directs network traffic to monitoring systems, such as intrusion detection and prevention sensors.

**Intrusion Detection System** Software that automates the intrusion detection process.

**Intrusion Prevention** The process of monitoring the events occurring in a computer system or network, analyzing them for signs of possible incidents, and attempting to stop detected possible incidents. See also "intrusion detection and prevention".

**Intrusion Prevention System** Software that has all the capabilities of an intrusion detection system and can also attempt to stop possible incidents. Also called an intrusion detection and prevention system.

**Invalid Web Pages** Sites where a domain may be registered but no content is served or the server is offline.

**Ipsec** Internet Protocol Security is a framework for a set of security protocols at the network or packet processing layer of network communications. IPsec is ubiquitous amongst firewall, VPNs, and routers.

**ISO/AISO** The persons responsible to the Office Head or Facility Director for ensuring that security is provided for and implemented throughout the life-cycle of an IT from the beginning of the concept development plan through its design, development, operation, maintenance, and secure disposal.

**Issue-Specific Policy** Policies developed to focus on areas of current relevance and concern to an office or facility. Both new technologies and the appearance of new threats often require the creation of issue-specific policies (email, Internet usage).

**IT Security** Measures and controls that protect an IT against denial of and unauthorized (accidental or intentional) disclosure, modification, or destruction of ITs and data. IT security includes consideration of all hardware and/or software functions.

**IT Security Policy** The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.

**IT Systems** An assembly of computer hardware, software and/or firmware configured to collect, create, communicate, compute, disseminate, process, store, and/or control data or information.

**Jamming** The deliberate radiation, re-radiation, or reflection of electromagnetic energy for the purpose of preventing or reducing an enemy's effective use of the electromagnetic spectrum, and with the intent of degrading or neutralizing the enemy's combat capability.

**Kerberos** Kerberos is a secret-key network authentication system developed by MIT and uses DES for encryption and authentication. Unlike a public-key authentication system, it does not produce digital signatures. Kerberos was designed to authenticate requests for network resources rather than to authenticate authorship of documents. See also: DSS.

**Key (digital)** A set of code synonymous with key pairs as part of a public key infrastructure. The key pairs include 'private' and 'public' keys. Public keys are generally used for encrypting data and private keys are generally used for signing and decrypting data.

**Key Distribution Center** A system that is authorized to transmit temporary session keys to principals (authorized users). Each session key is transmitted in encrypted form, using a master key that the key distribution shares with the target principal. See also: DSS, Encryption, Kerberos.

**Keystroke Logger** A device that monitors and records keyboard usage.

**Label** The marking of an item of information that reflects its information security classification. An internal label is the marking of an item of information that reflects the classification of that item within the confines of the medium containing the information. An external label is a visible or readable marking on the outside of the medium or its cover that reflects the security classification information resident within that particular medium. See also: Confidentiality.

**LAN (Local Area Network)** An interconnected system of computers and peripherals. LAN users can share data stored on hard disks in the network and can share printers connected to the network.

**Language** Content Filtering systems can be used to limit the results of an Internet search to those that are in your native language.

**LANL Unclassified Network** The LANL unclassified network that consists of two internal networks: the unclassified protected network (Yellow Network) and the open network (Green Network).

**LDAP** Short for Lightweight Directory Access Protocol, a set of protocols for accessing information directories. LDAP is based on the standards contained within the X.500 standard, but is significantly simpler. And unlike X.500, LDAP supports TCP/IP, which is necessary for any type of Internet access.

**Least Privilege** The principle that requires each subject be granted the most restrictive set of privileges needed for the performance of authorized tasks. The application of this principle limits the damage that can result from accident, error, or unauthorized use.

**Link Layer** Layer 2 in the OSI reference model. Responsible for moving data in and out across a physical link.

**Local Area Network** A short-haul data communications systems that connects IT devices in a building or group of buildings within a few square miles, including (but not limited to) workstations, front end processors, controllers, switches, and gateways.

**Macro Virus** A virus that attaches itself to application documents, such as word processing files and spreadsheets, and uses the application.s macro programming language to execute and propagate.

**Mail header** Filtering based solely on the analysis of e-mail headers. Antispam systems try to use this technique as well, but it is not very effective due to the ease of message header forgery.

**Mailing List** Used to detect mailing list messages and file them in appropriate folders.

**Major Application (MA)** A computer application that requires special management attention because of its importance to an organization's mission; its high development, operating, and/or maintenance costs; or its significant role in the administration of an organization's programs, finances, property, or other resources.

**Malicious Code/Virus** Sites that promote, demonstrate and/or carry malicious executable, virus or worm code that intentionally cause harm by modifying or destroying computer systems often without the user's knowledge.

**Malware** A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim.s data, applications, or operating system or of otherwise annoying or disrupting the victim.

**Management Controls** Security methods that focus on the management of the computer security system and the management of risk for a system.

**Management Information System (MIS)** An MIS is an assembly of computer hardware, software, and/or firmware configured to collect, create, communicate, compute, disseminate, process, store, and/or control data or information. Examples include: information storage and retrieval systems, mainframe computers, minicomputers, personal computers and workstations, office automation systems, automated message processing systems (AMPSs), and those supercomputers and process control computers (embedded computer systems) that perform general purpose computing functions.

**Management Network** A separate network strictly designed for security software management.

**Management Server** A centralized device that receives information from sensors or agents and manages them.

**Mass Mailing Worm** A worm that spreads by identifying e-mail addresses, often by searching an infected system, and then sending copies of itself to those addresses, either using the system.s e-mail client or a self-contained mailer built into the worm itself.

**Mechanisms** An assessment object that includes specific protection related items (hardware, software, or firmware) employed within or at the boundary of an information system.

**Memory Resident** A virus that stays in the memory of infected systems for an extended period of time.

**Microprocessor** A semiconductor central processing unit contained on a single integrated circuit chip.

**MIS Owner** The official who has the authority to decide on accepting the security safeguards prescribed for an MIS and is responsible for issuing an accreditation statement that records the decision to accept those safeguards. See also: Accreditation Approval (AA), Application Owner, Process Owner.

**MIS Security** Measures or controls that safeguard or protect an MIS against unauthorized (accidental or intentional) disclosure, modification, destruction of the MIS and data, or denial

of service. MIS security provides an acceptable level of risk for the MIS and the data contained in it. Considerations include: 1) all hardware and/or software functions, characteristics, and/or features; 2) operational procedures, accountability procedures, and access controls at all computer facilities in the MIS; 3) management constraints; 4) physical structures and devices; and 5) personnel and communications controls.

**Mission Assurance Category I (MAC I)** Systems handling information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. The consequences of loss of integrity or availability of a MAC I system are unacceptable and could include the immediate and sustained loss of mission effectiveness. MAC I systems require the most stringent protection measures.

**Mission Assurance Category II (MAC II)** Systems handling information that is important to the support of deployed and contingency forces. The consequences of loss of integrity are unacceptable. Loss of availability is difficult to deal with and can only be tolerated for a short time. The consequences could include delay or degradation in providing important support services or commodities that may seriously impact mission effectiveness or operational readiness. MAC II systems require additional safeguards beyond best practices to ensure assurance.

**Mission Assurance Category III (MAC III)** Systems handling information that is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short-term. The consequences of loss of integrity or availability can be tolerated or overcome without significant impacts on mission effectiveness or operational readiness. The consequences could include the delay or degradation of services or commodities enabling routine activities. MAC III systems require protective measures, techniques, or procedures generally commensurate with commercial best practices.

**Mobile Code** Software that is transmitted from a remote system to be executed on a local system, typically without the user.s explicit instruction.

**Modem** An electronic device that allows a microcomputer or a computer terminal to be connected to another computer via a telephone line.

**Multipartite Virus** A virus that uses multiple infection methods, typically infecting both files and boot sectors.

**Multiuser Systems** Any system capable of supporting more than one user in a concurrent mode of operation.

**National Computer Security Center (NCSC)** The government agency part of the National Security Agency (NSA) and that produces technical reference materials relating to a wide variety of computer security areas. It is located at 9800 Savage Rd., Ft. George G. Meade, Maryland.

**National Institute of Standards and Technology (NIST)** The federal organization that develops and promotes measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life.

**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 agency or by a contractor of an agency, or other organization on behalf of an agency—(i) 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 (ii) 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 Telecommunications and Information Systems Security Policy** Directs federal agencies, by July 15, 1992, to provide automated Controlled Access Protection (C2 level) for MIS, when all users do not have the same authorization to use the sensitive information.

**Need-to-Know** Access to information based on clearly identified need to know the information to perform official job duties.

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

**Network-Based Intrusion Prevention System** A program that performs packet sniffing and analyzes network traffic to identify and stop suspicious activity.

**Network-Based Intrusion Detection and Prevention System** An intrusion detection and prevention system that monitors network traffic for particular network segments or devices and analyzes the network and application protocol activity to identify and stop suspicious activity.

**Network Behavior Analysis System** An intrusion detection and prevention system that examines network traffic to identify and stop threats that generate unusual traffic flows.

**Network Layer** Layer 3 in the OSI reference model. Responsible for knowing the logical addresses of nodes, and for selecting routes through the network.

**Network Operations Center (NOC)** A location that monitors the operation of a network and usually provides efforts to solve connectivity and network problems. The NOC provides management of the terrestrial infrastructure by looking at configuration management and lock-down status/network systems monitoring. Network systems monitoring control sits in the NOC on the terrestrial side and monitors traffic to and from the terrestrial NOC.

**Network Security** Protection of networks and their services unauthorized modification, destruction, disclosure, and the

provision of assurance that the network performs its critical functions correctly and there are no harmful side-effects.

**Network Tap** A direct connection between a sensor and the physical network media itself, such as a fiber optic cable.

**Network Service Worm** A worm that spreads by taking advantage of a vulnerability in a network service associated with an operating system or an application.

**NIST** National Institute of Standards and Technology in Gaithersburg, Maryland. NIST publishes a wide variety of materials on computer security, including FIPS publications.

**Nonrepudiation** Method by which the sender is provided with proof of delivery and the recipient is assured of the sender's identity, so that neither can later deny having processed the data.

**Nonvolatile Memory Units** Devices which continue to retain their contents when power to the unit is turned off (bobble memory, Read-Only Memory/ROM).

**Obfuscation Technique** A way of constructing a virus to make it more difficult to detect.

**Object** A passive entity that contains or receives information. Access to an object potentially implies access to the information it contains. Examples of objects are records, blocks, pages, segments, files, directories, directory tree, and programs as well as bits, bytes, words, fields, processors, video displays, keyboards, clocks, printers, network nodes, etc.

**Object Reuse** The reassignment to some subject of a medium (e.g., page frame, disk sector, or magnetic tape) that contained one or more objects. To be securely reassigned, no residual data from previously contained object(s) can be available to the new subject through standard system mechanisms.

**Obscene/Tasteless** Sites that contain explicit graphical or text depictions of such things as mutilation, murder, bodily functions, horror, death, rude behavior, executions, violence, and obscenities etc. Sites which contain or deal with medical content *will not* be saved. Sample sites: www.celebritymorgue.com, www.rotten.com, and www.gruesome.com

**Offline** Pertaining to the operation of a functional unit when not under direct control of a computer. See also: Online.

**On-Access Scanning** Configuring a security tool to perform real-time scans of each file for malware as the file is downloaded, opened, or executed.

**On-Demand Scanning** Allowing users to launch security tool scans for malware on a computer as desired.

**Online** Pertaining to the operation of a functional unit when under the direct control of a computer. See also: Offline.

**Open Network** A network within the LANL Unclassified Network that supports LANL's public Internet presence and external collaborations. See LANL unclassified network.

**Open Systems Interconnection (OSI) Model** A standard reference model for communications between two hosts on a network.

**Operating System** The most important program that runs on a computer. Every general-purpose computer must have an operating system to run other programs. Operating systems perform basic tasks, such as recognizing input from the keyboard, sending output to the display screen, keeping track of files and directories on the disk, and controlling peripheral devices such as disk drives and printers.

**Operation Controls** Security methods that focus on mechanisms that primarily are implemented and executed by people (as opposed to systems).

**Operational Controls** The security controls (safeguards or countermeasures) for an information system that are primarily implemented and executed by people (as opposed to systems).

**Orange Book** Named because of the color of its cover, this is the DoD Trusted Computer System Evaluation Criteria, DoD 5200.28-STD. It provides the information needed to classify computer systems as security levels of A, B, C, or D, defining the degree of trust that may be placed in them. See also: C2, TCSEC.

**Organization** An entity of any size, complexity, or positioning within an organizational structure (a federal agency or, as appropriate, any of its operational elements).

**Organizational Computer Security Representative (OCSR)** A LANL person who has oversight responsibilities for one or more single-user, standalone classified or unclassified systems.

**Overwrite Procedure** A process, which removes or destroys data recorded on a computer storage medium by writing patterns of data over, or on top of, the data stored on the medium.

**Overwriting media** Method for clearing data from magnetic media. Overwriting uses a program to write (1s, 0s, or a combination) onto the media. Overwriting should not be confused with merely deleting the pointer to a file (which typically happens when a "delete" command is used).

**Parity** The quality of being either odd or even. The fact that all numbers have parity is commonly used in data communication to ensure the validity of data. This is called parity checking.

**Pass Code** A one-time-use "authenticator" that is generated by a token card after a user inputs his or her personal identification number (PIN) and that is subsequently used to authenticate a system user to an authentication server or workstation.

**Passive Fingerprinting** Analyzing packet headers for certain unusual characteristics or combinations of characteristics that are exhibited by particular operating systems or applications.

**Passive Sensor** A sensor that is deployed so that it monitors a copy of the actual network traffic.

**Password** A protected word, phrase, or string of symbols used to authenticate a user's identity to a system or network. Guidance note: One-time pass codes are valid only for a single authentication of a user to a system; reusable passwords are valid for repeated authentication of a user to a system.

**Payload** The portion of a virus that contains the code for the virus.s objective, which may range from the relatively benign (annoying people, stating personal opinions) to the highly malicious (forwarding personal information to others, wiping out systems).

**PBX** Short for private branch exchange, a private telephone network used within an enterprise. Users of the PBX share a

certain number of outside lines for making telephone calls external to the PBX.

**Penetration Testing** A test methodology in which assessors, using all available documentation (system design, source code, manuals) and working under specific constraints, attempt to circumvent the security features of an information system.

**Peripheral Device** Any external device attached to a computer. Examples of peripherals include printers, disk drives, display monitors, keyboards, and mice.

**Persistent Cookie** A cookie stored on a computer indefinitely so that a Web site can identify the user during subsequent visits.

**Personal Identification Number (PIN)** A number known only to the owner of the token card and which, once entered, generates a one-time pass-code.

**Personnel Security** The procedures established to ensure that all personnel who have access to any sensitive information have all required authorities or appropriate security authorizations.

**Phishing** Deceptive information pharming sites that are used to acquire personal information for fraud or theft. Typically found in hoax e-mail, these sites falsely represent themselves as legitimate Web sites to trick recipients into divulging user account information, credit-card numbers, usernames, passwords, Social Security numbers, etc. Pharming, or crimeware misdirects users to fraudulent sites or proxy servers, typically through DNS hijacking or poisoning.

**Phrases** Filtering based on detecting phrases in the content text and their proximity to other target phrases.

**Physical Layer** Layer 1 in the OSI reference model. Responsible for supporting the movement of bits on the physical medium.

**Physical Security** The application of physical barriers and control procedures as preventative measures or safeguards against threats to resources and information.

**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.

**Pornography/Adult Content** Sites that portray sexual acts and activity.

**Port** An interface on a computer to which you can connect a device.

**Port Protection Device** A device that authorizes access to the port itself, often based on a separate authentication independent of the computer's own access control functions.

**Precursor** A sign that a malware attack may occur in the future.

**Privacy Act of 1974** A US law permitting citizens to examine and make corrections to records the government maintains. It requires that Federal agencies adhere to certain procedures in their record keeping and interagency information transfers. See also: System of Records.

**Private Branch Exchange** Private Branch eXchange (PBX) is a telephone switch providing speech connections within an organization, while also allowing users access to both public switches and private network facilities outside the organization. The terms PABX, PBX, and PABX are used interchangeably.

**Process** An organizational assignment of responsibilities for an associated collection of activities that takes one or more kinds of input to accomplish a specified objective that creates an output that is of value.

**Process Owner** The official who defines the process parameters and its relationship to other Customs processes. The process owner has Accrediting Authority (AA) to decide on accepting the security safeguards prescribed for the MIS process and is responsible for issuing an accreditation statement that records the decision to accept those safeguards. See also: Application Owner.

**Promiscuous Mode** A configuration setting for a network interface card that causes it to accept all incoming packets that it sees, regardless of their intended destinations.

**Protected Distribution System (PDS)** A type of protected conduit system used for the protection of certain levels of information. PDS is the highest level of protection and is used in public domain areas for SRD and lower.

**Protected Transmission System** A cable, wire, conduit, or other carrier system used for the clear text transmission of classified information in certain DOE environments. Protected transmission systems comprise protected distribution systems (PDSs) and classified distributive information networks (CDINs). A wireline or fiber-optic telecommunications system that includes the acoustical, electrical, electromagnetic, and physical safeguards required to permit its use for the transmission of unencrypted classified information.

**Proxy** A program that receives a request from a client, and then sends a request on the client.s behalf to the desired destination.

**Public Law 100-235** Established minimal acceptable standards for the government in computer security and information privacy. See also: Computer Security Act of 1987.

**Quarantining** Storing files containing malware in isolation for future disinfection or examination.

**Radio Frequency (RF)** Any frequency within the electromagnetic spectrum normally associated with radio wave propagation. Organizations such as the Federal Communications Commission and International Telecommunication Union have divided the radio frequency spectrum into subdivisions for management purposes.

**RADIUS** Remote Authentication Dial-in User Service. A long-established de-facto standard whereby user profiles are maintained in a database that remote servers can share and authenticate dial-in users and authorize their request to access a system or service.

**Rainbow Series** A series of documents published by the National Computer Security Center (NCSC) to discuss in detail the features of the DoD, Trusted Computer System Evaluation Criteria (TCSEC) and provide guidance for meeting each requirement. The name "rainbow" is a nickname because each document has a different color of cover. See also: NCSC.

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

**Real Time** Occurring immediately. Real time can refer to events simulated by a computer at the same speed that they would occur in real life.

**Reciprocity** Mutual agreement among participating organizations to accept each other's security assessments in order to reuse information system resources and/or to accept each other's assessed security posture in order to share information.

**Records** The recordings (automated and/or manual) of evidence of activities performed or results achieved (forms, reports, test results), which serve as a basis for verifying that the organization and the information system are performing as intended. Also used to refer to units of related data fields (groups of data fields that can be accessed by a program and that contain the complete set of information on particular items).

**Recovery** The process of restoring an MIS facility and related assets, damaged files, or equipment so as to be useful again after a major emergency which resulted in significant curtailing of normal ADP operations. See also: Disaster Recovery.

**Regular Expression** Filtering based on rules written as regular expressions.

**Remanence** The residual information that remains on storage media after erasure. For discussion purposes, it is better to characterize magnetic remanence as the magnetic representation of residual information that remains on magnetic media after the media has been erased. The magnetic flux that remains in a magnetic circuit after an applied magnetomotive force has been removed. See also: Object Reuse.

**Remote Access** Sites that provide information about or facilitate access to information, programs, online services or computer systems remotely. Sample sites: pcnow.webex.com, and www.remotelyanywhere.com.

**Remote Administration Tool** A program installed on a system that allows remote attackers to gain access to the system as needed.

**Residual Risk** The risk of operating a classified information system that remains after the application of mitigating factors. Such mitigating factors include, but are not limited to minimizing initial risk by selecting a system known to have fewer vulnerabilities, reducing vulnerabilities by implementing countermeasures, reducing consequence by limiting the amounts and kinds of information on the system, and using classification and compartmentalization to lessen the threat by limiting the adversaries' knowledge of the system.

**Risk** The probability that a particular threat will exploit a particular vulnerability of the system.

**Risk Analysis** The process of identifying security risks, determining their magnitude, and identifying areas needing safeguards. An analysis of an organization's information resources, its existing controls, and its remaining organizational and MIS 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. See also: Risk Assessment, Risk Management.

**Risk Assessment** Process of analyzing threats to and vulnerabilities of an MIS to determine the risks (potential for losses), and using the analysis as a basis for identifying appropriate and cost-effective measures. See also: Risk Analysis, Risk Management. Risk analysis is a part of risk management, which is used to minimize risk by specifying security measures commensurate with the relative values of the resources to be protected, the vulnerabilities of those resources, and the identified threats against them. The method should be applied iteratively during the system lifecycle. When applied during the implementation phase or to an operational system, it can verify the effectiveness of existing safeguards and identify areas in which additional measures are needed to achieve the desired level of security. There are numerous risk analysis methodologies and some automated tools available to support them.

**Risk Executive (Function)** An individual or group within an organization that helps to ensure that: (i) security risk-related considerations for individual information systems, to include the authorization decisions, are viewed from an organization wide perspective with regard to the overall strategic goals and objectives of the organization in carrying out its missions and business functions; and (ii) managing information system-related security risks is consistent across the organization, reflects organizational risk tolerance, and is considered along with other organizational risks affecting mission/business success.

**Risk Management** The total process of identifying, measuring, controlling, and eliminating or minimizing uncertain events that may affect system resources. Risk management encompasses the entire system life-cycles and has a direct impact on system certification. It may include risk analysis, cost/benefit analysis, safeguard selection, security test and evaluation, safeguard implementation, and system review. See also: Risk Analysis, Risk Assessment.

**Router** An interconnection device that is similar to a bridge but serves packets or frames containing certain protocols. Routers link LANs at the network layer.

**ROM** Read Only Memory. See also: Nonvolatile Memory Units.

**Rootkit** A collection of files that is installed on a system to alter the standard functionality of the system in a malicious and stealthy way.

**Route Hijacking** A routing-based denial of service attack involves attackers manipulating routing table entries to deny service to legitimate systems or networks.

**RSA** A public-key cryptosystem for both encryption and authentication based on exponentiation in modular arithmetic. The algorithm was invented in 1977 by Rivest, Shamir, and Adelman and is generally accepted as practical or secure for public-key encryption. See also: Capstone, Clipper, DES, RSA, Skipjack.

**Rules of Behavior** Rules 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 work 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.

**Safeguards** Countermeasures, specifications, or controls, consisting of actions taken to decrease the organizations existing degree of vulnerability to a given threat probability, that the threat will occur.

**Satellites** Craft positioned hundreds to thousands of miles in space to efficiently relay a wide variety of broadcast and two-way communications across great distances.

**Satellite Communications (SATCOM)** A satellite communications system is comprised of three segments: Space Segment, Control Segment, and Terminal (Ground) Segment.

**Satellite Control Stations** Monitor satellite health and command the mission operations and maintenance functions of satellites and system components. Satellite control stations are typically divided into the SOC and the NOC.

**Satellite Operations Center (SOC)** One or more facilities that supports space segment operations by providing pre-launch planning, launch and early orbit support, and satellite control functions. SOC personnel perform satellite command and control during launch, on-orbit test, and deployment, and assist in major anomaly resolution.

**Security Incident** An MIS security incident is any event and/or condition that has the potential to impact the security and/or accreditation of an MIS and may result from intentional or unintentional actions. See also: Security Violation.

**Security Authorization** See: *Authorization*.

**Security Categorization** The process of determining the security category for information or an information system. Security categorization methodologies are described in CNSS Instruction 1253 for national security systems and in FIPS 199 for other than national security systems.

**Security Control Assessment** The testing and/or evaluation of the management, operational, and technical security controls in an information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

**Security Control Assessor** The individual, group, or organization responsible for conducting a security control assessment.

**Security Control Baseline** One of the sets of minimum security controls defined for federal information systems in NIST Special Publication 800-53 and CNSS Instruction 1253.

**Security Control Enhancements** Statements of security capability to: (i) build in additional, but related, functionality to a basic control; and/or (ii) increase the strength of a basic control.

**Security Control Inheritance** A situation in which an information system or application receives protection from security controls (or portions of security controls) that are developed, implemented, assessed, authorized, and monitored by entities other than those responsible for the system or application; entities either internal or external to the organization where the system or application resides. See: *Common Control*.

**Security Controls** The management, operational, and technical controls (safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

**Security Impact Analysis** The analysis conducted by an organizational official to determine the extent to which changes to the information system have affected the security state of the system.

**Security Objective** Confidentiality, integrity, or availability.

**Security Plan** Document that details the security controls established and planned for a particular system.

**Security Policy** The set of laws, rules, directives, and practices that regulate how an organization manages, protects, and distributes controlled information.

**Security Requirements** Types and levels of protection necessary for equipment, data, information, applications, and facilities to meet security policies.

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

**Security Specifications** A detailed description of the security safeguards required to protect a system.

**Security Violation** An event, which may result in disclosure of sensitive information to, unauthorized individuals, or that results in unauthorized modification or destruction of system data, loss of computer system processing capability, or loss or theft of any computer system resources. See also: Security Incident.

**Senior Agency Information Security Officer** Official responsible for carrying out the Chief Information Officer responsibilities under FISMA and serving as the Chief Information Officer's primary liaison to the agency's authorizing officials, information system owners, and information system security officers. [Note: Organizations subordinate to federal agencies may use the term *Senior Information Security Officer* or *Chief Information SecurityOfficer* to denote individuals filling positions with similar responsibilities to Senior Agency Information Security Officers.]

**Senior Information Security Officer** See: *Senior Agency Information Security Officer*.

**Sensitive Data** Any information, the loss, misuse, modification of, or unauthorized access to, could affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, U.S. Code, but has not been specifically authorized under criteria established by an Executive order or an act of Congress to be kept classified in the interest of national defense or foreign policy.

**Sensitive Unclassified Information** Information for which disclosure, loss, misuse, alteration, or destruction could adversely affect national security or other federal government interests. Guidance Note: National security interests are those unclassified matters that relate to the national

defense or to United States (US) foreign relations. Other government interests are those related to, but not limited to, a wide range of government or government-derived economic, human, financial, industrial, agricultural, technological, and law-enforcement information, and to the privacy or confidentiality of personal or commercial proprietary information provided to the U.S. government by its citizens. Examples are Unclassified Controlled Nuclear Information (UCNI), Official Use Only (OUO) information, Naval Nuclear Propulsion Information (NNPI), Export Controlled Information (ECI), In Confidence information, Privacy Act information (such as personal/medical information), proprietary information, for example, from a cooperative research and development agreement (CRADA), State Department Limited Official Use (LOU) information, and Department of Defense For Official Use Only (FOUO) information.

**Sensitivity Level** Sensitivity level is the highest classification level and classification category of information to be processed on an information system.

**Sensor** An intrusion detection and prevention system component that monitors and analyzes network activity and may also perform prevention actions.

**Separation of Duties** The dissemination of tasks and associated privileges for a specific computing process among multiple users to prevent fraud and errors.

**Server** The control computer on a local area network that controls software access to workstations, printers, and other parts of the network.

**Session Cookie** A temporary cookie that is valid only for a single Web site session.

**Shim** A layer of host-based intrusion detection and prevention code placed between existing layers of code on a host that intercepts data and analyzes it.

**Signature** A set of characteristics of known malware instances that can be used to identify known malware and some new variants of known malware.

**Signature-Based Detection** The process of comparing signatures against observed events to identify possible incidents.

**Site** Usually a single physical location, but it may be one or more MIS that are the responsibility of the DSO. The system may be a standalone MIS, a remote site linked to a network, or workstations interconnected via a local area network (LAN).

**Skipjack** A classified NSA designed encryption algorithm contained in the Clipper Chip. It is substantially stronger than DES and intended to provide a federally mandated encryption process, which would enable law enforcement agencies to monitor and wiretap private communications. See also: Capstone, Clipper, DES, RSA, Skipjack.

**Smart Card** A credit-card – sized device with embedded microelectronics circuitry for storing information about an individual. This is not a key or token, as used in the remote access authentication process.

**SNMP** Simple Networking Management Protocol.

**Software** Computer instructions or data. Anything that can be stored electronically is software.

**Software Copyright** The right of the copyright owner to prohibit copying and/or issue permission for a customer to employ a particular computer program.

**Space Segment** There are two parts to the space segment: ground elements and satellite(s), each comprised of platform (the basic structure and subsystems of the satellite) and payload. The payload provides space-based capabilities to the users and distinguishes one type of satellite from another.

**SPAM** To crash a program by overrunning a fixed-site buffer with excessively large input data. Also, to cause a person or newsgroup to be flooded with irrelevant or inappropriate messages.

**Spanning Port** A switch port that can see all network traffic going through the switch.

**Specification** An assessment object that includes document-based artifacts (policies, procedures, plans, system security requirements, functional specifications, and architectural designs) associated with an information system.

**Spyware** Sites that promote, offer or secretively install software to monitor user behavior, track personal information, record keystrokes, and/or change user computer configuration without the user's knowledge and consent malicious or advertising purposes. Includes sites with software that can connect to "phone home" for transferring user information.

**Spyware Detection and Removal Utility** A program that monitors a computer to identify spyware and prevent or contain spyware incidents.

**Standard Security Procedures** Step-by-step security instructions tailored to users and operators of MIS that process sensitive information.

**Standalone System** A single-user MIS not connected to any other systems.

**Stateful Protocol Analysis** The process of comparing predetermined profiles of generally accepted definitions of benign protocol activity for each protocol state against observed events to identify deviations.

**Stealth Mode** Operating an intrusion detection and prevention sensor without IP addresses assigned to its monitoring network interfaces.

**Subsystem** A major subdivision or component of an information system consisting of information, information technology, and personnel that performs one or more specific functions.

**Supplementation (Assessment Procedures)** The process of adding assessment procedures or assessment details to assessment procedures in order to adequately meet the organization's risk management needs.

**Supplementation (Security Controls)** The process of adding security controls or control enhancements to a security control baseline from NIST Special Publication 800-53 or CNSS Instruction 1253 in order to adequately meet the organization's risk management needs.

**Symmetric Encryption** See: Conventional Encryption.

**System** An organized hierarchy of components (hardware, software, data, personnel, and communications, for example) having a specified purpose and performance requirements.

**System Administrator** The individual responsible for the installation and maintenance of an information system, providing effective information system utilization, required security parameters, and implementation of established requirements.

**System Availability** The state that exists when required automated informations can be performed within an acceptable time period even under adverse circumstances.

**System Failure** An event or condition that results in a system failing to perform its required function.

**System Integrity** The attribute of a system relating to the successful and correct operation of computing resources. See also: Integrity.

**System of Records** A group of any records under the control of the Department from which information is retrieved by the name of an individual, or by some other identifying number, symbol, or other identifying particular assigned to an individual. See also: Privacy Act of 1974.

**System Owner** The person, team, group, or division that has been assigned and accepted responsibility for Laboratory computer assets.

**System Recovery** Actions necessary to restore a system's operational and computational capabilities, and its security support structure, after a system failure or penetration.

**System Security Plan** Formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.

**System-Specific Security Control** A security control for an information system that has not been designated as a common control or the portion of a hybrid control that is to be implemented within an information system.

**System User** An individual who can receive information from, input information to, or modify information on a LANL information system without an independent review. Guidance Note: This term is equivalent to computer information system user, or computer user, found in other Laboratory documentation. System users may be both LANL workers and collaborators. For desktop systems, a single individual may be a system user and system owner.

**Tailoring** The process by which a security control baseline is modified based on: (i) the application of scooping guidance; (ii) the specification of compensating security controls, if needed; and (iii) the specification of organization-defined parameters in the security controls via explicit assignment and selection statements.

**Tailoring (Assessment Procedures)** The process by which assessment procedures defined in Special Publication 800-53A are adjusted, or scoped, to match the characteristics of the information system under assessment, providing organizations with the flexibility needed to meet specific organizational requirements and to avoid overly-constrained assessment approaches.

**Tailored Security Control Baseline** A set of security controls resulting from the application of tailoring guidance to the security control baseline. See *Tailoring*.

**TCP/IP** Transmission Control Protocol/Internet Protocol. The Internet Protocol is based on this suite of protocols.

**TCSEC** Trusted Computer System Evaluation Criteria (TCSEC). DoD 5200.28-STD, National Institute of Standards and Technology (NIST), Gaithersburg, Maryland, 1985. Establishes uniform security requirements, administrative controls, and technical measures to protect sensitive information processed by DoD computer systems. It provides a standard for security features in commercial products and gives a metric for evaluating the degree of trust that can be placed in computer systems for the securing of sensitive information. See also: C2, Orange Book.

**Technical Controls** Security methods consisting of hardware and software controls used to provide automated protection to the system or applications. Technical controls operate within the technical system and applications.

**Technical Security Policy** Specific protection conditions and/or protection philosophy that express the boundaries and responsibilities of the IT product in supporting the information protection policy control objectives and countering expected threats.

**Telecommunications** Any transmission, emission, or reception of signals, writing, images, sound or other data by cable, telephone lines, radio, visual or any electromagnetic system.

**Terminal (Ground) Segment** This segment comprises the actual equipment that receives and transmits signals to the satellite. Terminals can vary from a hand-held or man-pack terminal to a large fixed installation.

**Terrestrial Data Links** Network connections that tie together the control stations, ground stations, and the rest of the terrestrial telecommunications infrastructure.

**Terrorist/Militant/Extremist** Sites that contain information regarding militias, anti-government groups, terrorism, anarchy, etc.: Anti-government/Anti-establishment and bomb-making/usage (Should also be saved in criminal skills). Sample sites: www.michiganmilitia.com, www.militiaofmontana.com, and www.ncmilitia.org.

**Test** A type of assessment method that is characterized by the process of exercising one or more assessment objects under specified conditions to compare actual with expected behavior, the results of which are used to support the determination of security control effectiveness over time.

**Test Condition** A statement defining a constraint that must be satisfied by the program under test.

**Test Data** The set of specific objects and variables that must be used to demonstrate that a program produces a set of given outcomes. See also: Disaster Recovery, Test Program.

**Test Plan** A document or a section of a document which describes the test conditions, data, and coverage of a particular test or group of tests. See also: Disaster Recovery, Test Condition, Test Data, Test Procedure (Script).

**Test Procedure (Script)** A set of steps necessary to carry out one or a group of tests. These include steps for test environment initialization, test execution, and result analysis. The test procedures are carried out by test operators.

**Test Program** A program which implements the test conditions when initialized with the test data and which collects the results produced by the program being tested. See also: Disaster Recovery, Test Condition, Test Data, Test Procedure (Script).

**The Computer Security Plans for General Support Systems (GSS) and Major Applications (MA)** Plans that detail the specific protection requirements for major applications and general support systems.

**The Cyber Security Handbook** A Web-site handbook that details the Cyber Security requirements required by system

users, system administrators, and SRLMs who access electronic information.

**Threat** An event, process, activity (act), substance, or quality of being perpetuated by one or more threat agents, which, when realized, has an adverse effect on organization assets, resulting in losses attributed to: direct loss, related direct loss, delays or denials, disclosure of sensitive information, modification of programs or databases and intangible (good will, reputation, etc.).

**Threat Agent** Any person or thing, which acts, or has the power to act, to cause, carry, transmit, or support a threat. See also: Threat.

**Threat Assessment** Process of formally evaluating the degree of threat to an information system or enterprise and describing the nature of the threat.

**Threat Source** The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability. Synonymous with threat agent.

**Threshold** A value that sets the limit between normal and abnormal behavior.

**Token Card** A device used in conjunction with a unique PIN to generate a one-time pass code (for example, CRYPTOCard® or SecureID)®).

**Tracking Cookie** A cookie placed on a user.s computer to track the user.s activity on different Web sites, creating a detailed profile of the user.s behavior.

**Transmission Security (TRANSEC)** Component of COMSEC resulting from the TRANSEC application of measures designed to protect transmissions from interception and exploitation by means other than cryptanalysis.

**Transport Layer** Layer 4 of the OSI reference model. Ensures the reliable delivery of messages and provides error-checking mechanisms.

**Trapdoor** A secret undocumented entry point into a computer program, used to grant access without normal methods of access authentication. See also: Malicious Code.

**Triangulation** Identifying the physical location of a detected threat against a wireless network by estimating the threat's approximate distance from multiple wireless sensors by the strength of the threat's signal received by each sensor, then calculating the physical location at which the threat would be the estimated distance from each sensor.

**Trigger** A condition that causes a virus payload to be executed, usually occurring through user interaction (opening a file, running a program, clicking on an e-mail file attachment).

**Trojan Horse** A computer program with an apparently or actually useful function that contains additional (hidden) functions that surreptitiously exploit the legitimate authorizations of the invoking process to the detriment of security. See also: Malicious Code. Threat Agent.

**Trusted Computer Base (TCB)** The totality of protection mechanisms within a computer system, including hardware, firmware, and software, the combination of which is responsible for enforcing a security policy. A TCB consists of one or more components that together enforce a security policy over a product or system. See also: C2, Orange Book, TCSEC.

**Trusted Computing System** A computer and operating system that employs sufficient hardware and software integrity measures to allow its use for simultaneously processing a range of sensitive information and can be verified to implement a given security policy.

**Tuning** Altering the configuration of an intrusion detection and prevention system to improve its detection accuracy.

**Unclassified Cyber Security Program Plan** A plan that provides a single source of unclassified computer security program information, and specifies the minimum protections and controls and references the detailed source material that pertains to the program.

**Unclassified Information Systems Security Site Manager** The manager responsible for the LANL Unclassified Information Systems Security Program.

**Unclassified Protected Network** A network within the LANL unclassified network that is designed to protect the resident systems from unauthorized access and is separated from the Internet by a firewall that controls external access to the network. See also: LANL Unclassified Network.

**Unfriendly Termination** The removal of an employee under involuntary or adverse conditions. This may include termination for cause, RIF, involuntary transfer, resignation for "personality conflicts," and situations with pending grievances.

**Uplink** The portion of a communications link used to transmit signals from an Earth-based terminal (on land, ship, or aircraft) to a satellite.

**UPS (Uninterruptible Power Supply)** A system of electrical components to provide a buffer between utility power, or other power source, and a load that requires uninterrupted, precise power. This often includes a trickle-charge battery system which permits a continued supply of electrical power during brief interruption (blackouts, brownouts, surges, electrical noise, etc.) of normal power sources.

**User** Any person who is granted access privileges to a given IT.

**User Interface** The part of an application that the user works with. User interfaces can be text-driven, such as DOS, or graphical, such as Windows.

**Verification** The process of comparing two levels of system specifications for proper correspondence.

**Very Small Aperture Terminal (VSAT)** Refers to small Earth station employing a satellite antenna with a diameter or cross-section dimension in the general range of 1.2 to 2.4 meters. VSAT terminals are used in networks that primarily support point-to-multipoint communications as part of large private networks, particularly in large retail networks to support transactions such as inventory management and credit-card authorizations.

**Virus** Code imbedded within a program that causes a copy of itself to be inserted in one or more other programs. In addition to propagation, the virus usually performs some unwanted function. Note that a program need not perform malicious actions to be a virus; it need only infect other programs. See also: Malicious Code.

**VSAN** Virtual SAN.

**Vulnerability** A weakness, or finding that is non-compliant, non-adherent to a requirement, a specification or a standard,

or unprotected area of an otherwise secure system, which leaves the system open to potential attack or other problem.

**WAN (Wide Area Network)** A network of LANs, which provides communication, services over a geographic area larger than served by a LAN.

**Web Browser Plug-In** A mechanism for displaying or executing certain types of content through a Web browser.

**Web Bug** A tiny graphic on a Web site that is referenced within the Hypertext Markup Language (HTML) content of a Web page or e-mail to collect information about the user viewing the HTML content.

**Whitelist** A list of discrete entities, such as hosts or applications, that are known to be benign.

**Wireless Intrusion Detection and Prevention System** An intrusion detection and prevention system that monitors wireless network traffic and analyzes its wireless networking protocols to identify and stop suspicious activity involving the protocols themselves.

**World Wide Web** An association of independent information databases accessible via the Internet. Often called the Web, WWW, or W.

**Worm** A computer program that can replicate itself and send copies from computer to computer across network connections. Upon arrival, the worm may be activated to replicate and propagate again. In addition to propagation, the worm usually performs some unwanted function. See also: Malicious Code.

**Worms** Worms are a type of virus that consume memory and network bandwidth, and can ultimately cause a computer to stop responding. Worms can permit an attacker to access computers remotely and require no user action to spread.

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

**WWW** See: World Wide Web.

**Yellow Network** See LANL Unclassified Network.

**Zombie** A program that is installed on a system to cause it to attack other systems.