U.S. NUCLEAR REGULATORY COMMISSION

DIRECTIVE TRANSMITTAL

TN: DT-94-08

To:	NRC Management Directives Custodians
Subject:	Transmittal of Volume 12, "Glossary"
Purpose:	The revision to the Volume 12 Glossary defines certain terms relating to the processing of personnel security clearances (MD 12.3) that were previously defined only in other reference documents.
Office and Division of Origin:	Office of Administration Division of Security
Contact:	Lewis Robertson/James J. Dunleavy, 415-6540
Date Approved:	July 15, 1994
Volume:	12 Security
Directive:	12 "Glossary"
Availability:	U.S. Government Printing Office, (202) 512-2409

Glossary

Volume 12

Glossary[1] Volume 12

The following definitions are written from the viewpoint of their specialized meaning in security documents.

Access Authorization. An administrative determination that an individual (including a consultant) who is employed by, or is an applicant for employment with, the NRC, NRC contractors, agents, and licensees of the NRC, or other person designated by the Executive Director for Operations, is eligible for a security clearance for access to Restricted Data, Formerly Restricted Data, or National Security Information.

Accountable Communications Security (COMSEC) Material. All COMSEC aids, equipments, and components thereof, and devices that are identifiable by the telecommunications security (TSEC) nomenclature system, for example, KG-36, KAG-25, or a comparable system of another U.S. department or agency, foreign government, or international organization. (See also Communications Security.)

Accreditation. The authorization and approval granted to a system or network to process classified and/or sensitive unclassified data in an operational environment made on the basis of a certification by the designated security officers to the extent that design and implementation of the system meet prespecified technical requirements for achieving adequate security.

Administrative Security. The management constraints, operational procedures, and supplemental controls established to provide an acceptable level of protection for sensitive data. (See also Automated Data Processing (ADP) Security, Communications Security, Data Security, Physical Security, Teleprocessing Security, and Transmission Security.)

Agency Communications Security (COMSEC) Custodian. The individual designated to coordinate all NRC COMSEC accounts and to be responsible for the Central Office of Record.

[1]This Glossary applies to all directives pertaining to Security in Volume 12.

Glossary (continued)

Application System. A collection of one or more related computer programs designed to solve a particular problem or to perform a distinct agency function.

Audit. To conduct the independent review and examination of system records and activities in order to test for adequacy of system controls, to ensure compliance with established policy and operational procedures, and to recommend any indicated changes in controls, policy, or procedures.

Audit Trail. A manual or automated means of tracing the processing steps within an ADP system.

Authentication.

1. The act of identifying or verifying the eligibility of a station, an originator, or an individual to access specific categories of information.

2. A measure designed to provide protection against fraudulent transmissions by establishing the validity of a transmission, a message, a station, or an originator.

Authorized Classifier. An individual authorized in writing by appropriate authority to classify, declassify, or downgrade information. This term applies to derivative classifiers and original classifiers.

Automated Data Processing (ADP) Access Controls. Hardware or software features, operating procedures, management procedures, and various combinations thereof, designed to detect and prevent unauthorized access and to permit authorized access to an ADP system.

Automated Data Processing (ADP) Facility. One or more rooms of a building containing the main elements of an ADP system.

Automated Data Processing (ADP) Security. The hardware/software functions, characteristics, and features; operational procedures, accountability procedures, and access controls at the central computer facility, remote computer, and terminal facilities; the management constraints, physical structure, and devices; and personnel and telecommunications controls needed to provide an

Glossary (continued)

Automated Data Processing (ADP) Security (continued)

acceptable level of protection to a computer system. (See also Administrative Security, Communications Security, Data Security, Physical Security, Teleprocessing Security, and Transmission Security.)

Automated Data Processing (ADP) System. An assembly of computer equipment, facilities, personnel, software, and procedures configured for the purpose of classifying, sorting, calculating, computing, summarizing, storing, and retrieving data and information with a minimum of human intervention. An ADP system includes general-purpose and special-purpose computers; commercially available components; auxiliary, accessory, or peripheral equipment; and electrical accounting machines.

Automated Decisionmaking System. Computer applications that issue checks, requisition supplies, or perform similar functions based on programmed criteria, with little human intervention.

Automated Information System (also referred to as automated system). An assembly of procedures, processes, methods, routines, or techniques (including but not limited to systems such as payroll, personnel, and property and supply) united by some form of regulated interaction to form an organized whole specifically designed to make use of ADP equipment.

Automated Security Monitoring. The use of automated procedures to ensure that the security controls implemented within an ADP system are not circumvented.

Automated System Security Integrity Study. An analysis, test, and evaluation of the security measures of an automated system, including its administrative, automated, and physical security measures, to evaluate the ability of the measures to protect classified data.

Automated System Security Proposal. A proposal that outlines an automated system and the security measures to protect classified and/or sensitive unclassified data processed or produced by the system. Once approved, the proposal becomes a plan.

Glossary (continued)

Automatic Answering Mode. Answering in which the called data terminal equipment automatically responds to the calling signal. The call may be established whether or not the data terminal equipment is attended.

Backup Procedures. The provisions made for the recovery of data files and program libraries and for restart or replacement of ADP equipment after a system failure or the occurrence of a disaster.

Browsing. Searching through storage to locate or acquire information, without necessarily knowing of the existence or the format of the information being sought.

Call Back. A procedure established for positively identifying a terminal dialing into a computer system by disconnecting the calling terminal and reestablishing the connection by the computer system's dialing the telephone number of the calling terminal.

CCI. See Controlled Cryptographic Item.

Central Office of Record (COR). The activity within a department or agency charged with responsibility for maintaining records of accountability of all accountable COMSEC material received by or generated within the department or agency.

Certification. The technical evaluation made as part of and in support of the accreditation process that establishes the extent to which a particular computer system or network design and implementation meet a prespecified set of security requirements.

Classification. A term applied collectively to original classification and derivative classification.

Classification Authority. The authorized classifier, the classification guide, or the source document or documents that determine the classification of information.

Classification Guide. A document issued by an original classification authority that provides derivative classification instructions.

Classified Data. Restricted Data, Formerly Restricted Data, and National Security Information processed or produced by a system that requires protection against unauthorized disclosure in the interest of national security.

Glossary (continued)

Classified Information. Information (such as a document or correspondence) that is designated National Security Information, Restricted Data, or Formerly Restricted Data.

Classified Interest. Classified information possessed by NRC, an NRC contractor, or by any other facility.

Classified Safeguards Information. Certain types of information relating to the safeguarding of nuclear material or facilities classified as National Security Information or Restricted Data in accordance with the provisions of the "Classification Guide for National Security Information Concerning Nuclear Materials and Facilities" and to other information not specifically mentioned in the guide but referenced in supplementary memoranda, bulletins, or guides.

Collateral Intelligence. Non-SCI (sensitive compartmented information) intelligence.

Commission. The Nuclear Regulatory Commission of five members or a quorum thereof sitting as a body, as provided by Section 201 of the Energy Reorganization Act of 1974, as amended.

Communications Center. See Secure Telecommunications Facility.

Communications Link. The physical means, for example, a telephone line, of connecting one location to another for the purpose of transmitting information.

Communications Protection. Applying special measures, such as the data encryption standard (DES) and call-back techniques, to protect sensitive unclassified telecommunications in order to deny unauthorized persons unclassified information of value, to prevent disruption, or to ensure the authenticity of such telecommunications.

Communications Security (COMSEC). The protective measures taken to deny unauthorized persons information derived from telecommunications of the United States Government related to national security and to ensure the authenticity of any such communications. Such protection results from the application of security measures (including cryptosecurity, transmission security, and emissions security) to electrical systems generating, handling,

Glossary (continued)

Communications Security (COMSEC) (continued)

processing, or using National Security Information. It also includes the application of physical security measures to communications security information or materials. (See also Administrative Security, ADP Security, Data Security, Physical Security, Teleprocessing Security, and Transmission Security.)

Compartmentalization (ADP).

1. The isolation of the operating system, user programs, and data files from one another in main storage in order to provide protection against unauthorized or concurrent access by other users or programs.
2. The breaking down of sensitive data into small, isolated blocks for the purpose of reducing risk to the data.

Compromise. The disclosure of classified information or administratively controlled information to persons not authorized to receive such information.

Compromising Emanations (TEMPEST). Unintentional intelligence-bearing signals that if intercepted and analyzed disclose classified information being transmitted, received, handled, or otherwise processed by any information-processing system.

Computer Center. One or more computers with their peripheral and storage units, central processing units, and communications equipment in a single controlled area. The term "computer center" might also be referred to as the ADP facility, the ADP installation, the ADP center, or the ADP installation/center.

Computer Program. The sequence of coded instructions that cause the computer to solve a problem or perform an ADP operation.

COMSEC. See Communications Security.

COMSEC Account. An administrative entity, identified by an account number, responsible for maintaining custody and control of COMSEC material.

COMSEC Accounting. Procedures by which control of COMSEC material is maintained from time of origin through destruction or final disposition.

Glossary (continued)

COMSEC Control Officer. The individual designated by the supervisor of a secure communications facility to be in charge of the day-to-day operations of the facility.

COMSEC Custodian. The individual designated to be responsible for the receipt, transfer, accountability, safeguarding, and destruction of COMSEC material issued to a COMSEC account.

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

COMSEC Facility. A facility that contains classified COMSEC material.

COMSEC Information. All information concerning COMSEC and all COMSEC material.

COMSEC Insecurity. Any occurrence that jeopardizes the security of COMSEC material or the secure electrical transmission of National Security Information or national security-related information.

COMSEC Material. COMSEC aids, equipment, and components thereof, and devices that are identifiable by the telecommunications security (TSEC) nomenclature system or a similar system of a U.S. department or agency, foreign government, or international organization.

COMSEC Measures. All cryptographic, transmission security, emission security, and physical security techniques employed to protect telecommunications.

COMSEC Survey.

1. The application of COMSEC analysis and assessment techniques to a specific operation, function, or program.

Glossary (continued)

COMSEC Survey (continued)

2. Examination and inspection of a physical location to determine whether alterations and modifications are necessary to render it acceptable for the installation and operation of COMSEC equipment.

COMSEC System. The combination of all measures intended to provide communications security for a specific telecommunications system, including associated cryptographic, transmission, emission, computer, and physical security measures, as well as the COMSEC support system (documentation; doctrine; keying material protection and distribution; and equipment engineering, production, distribution, modification, and maintenance).

CONFIDENTIAL. The classification level applied to information the unauthorized disclosure of which could reasonably be expected to cause damage to the national security. (The lowest level of classification.)

Confidential Source. Any individual or organization that has provided or that may reasonably be expected to provide information to the United States on matters pertaining to the national security or law enforcement with the expectation, expressed or implied, that the information or relationship, or both, be held in confidence.

Contingency Plans. Plans for emergency response, backup operations, and postdisaster recovery.

Controlled Area. An area over which NRC or an NRC contractor exercises administrative and physical control by use of properly cleared and authorized employees or guards stationed so as to control admittance to the room, building, or structure or by use of a lock that provides reasonable protection against surreptitious entry.

Controlled Cryptographic Item (CCI). Any material that is accountable in a COMSEC inventory under the control of a COMSEC custodian.

Glossary (continued)

Control Zone. The space, expressed in feet of radius, that surrounds equipment that is used to process sensitive information and that is under sufficient physical and technical control to preclude an unauthorized entry or compromise. Synonymous with security perimeter.

COR. See Central Office of Record.

Counterintelligence. Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations for or on behalf of foreign powers, organizations, or persons, or international terrorist activities, but not including security programs for personnel, physical security, documents, or communications.

Countermeasure. An action, procedure, modification, or physical device that is applied to reduce or inhibit the generation of compromising emanations.

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

Cryptanalysis. The steps and operations performed in converting encrypted messages into plain text without initial knowledge of the key employed in the encryption. In COMSEC, the purpose of cryptanalysis is to evaluate the adequacy of the security protection that it is intended to provide, or to discover weaknesses or vulnerabilities that could be exploited to defeat or lessen that protection.

CRYPTO. A marking or designator identifying all COMSEC keying material used to protect or authenticate telecommunications carrying National Security Information and national security-related information.

Crypto-Equipment. Any equipment employing a cryptographic logic.

Cryptographic. Pertaining to or concerned with cryptography.

Cryptographic System. See Cryptosystem.

Glossary (continued)

Cryptography.

1. The protection of telecommunications by rendering information unintelligible or unrecognizable until it reaches the intended recipient.
2. The design and use of cryptosystems.

Crypto-Information. Information that would make a significant contribution to the cryptoanalytic solution of encrypted text of a cryptosystem.

Crypto-Insecurity. An equipment malfunction or an operator error that adversely affects the security of a cryptosystem.

Cryptology. The field that encompasses both cryptography and cryptanalysis.

Cryptomaterial. All material, including documents, devices, or equipment, that contains crypto-information and is essential to the encryption, decryption, or authentication of telecommunications.

Cryptosecurity. The component of communications security that results from the provision of technically sound cryptosystems and their proper use.

Cryptosystem. The associated items of COMSEC equipment or material used as a unit to provide a single means of encryption and decryption.

Cryptovariable. See Keying Material.

Custodian. Any person to whom classified information is charged by records of the NRC or of its contractors, or in the case of CONFIDENTIAL information in the absence of records, any person who possesses the information.

Data-Dependent Protection. Protection of data at a level commensurate with the sensitivity level of the individual data elements, rather than with the sensitivity of the entire file that includes the data elements.

Data Encryption Standard (DES). An unclassified crypto-algorithm published by the National Institute of Standards and Technology in FIPS PUB 46 for the protection of certain U.S. Government information.

Glossary (continued)

Data Security. The protection of data from accidental or malicious modification, destruction, or disclosure. (See also ADP Security, Communications Security, Physical Security, Teleprocessing Security, and Transmission Security.)

Decipher. To convert enciphered text to plain text by means of a cipher system.

Declassification.

1. A determination by appropriate authority that information no longer requires classification protection; or
2. A determination by appropriate authority in accordance with approved classification policy or guidance that a classified document is no longer classified; or
3. The removal of classification markings from a document in accordance with a declassification notice from an appropriate authority.

Decrypt. To convert encrypted text into its equivalent plain text by means of a cryptosystem.

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

Degauss. To apply a variable alternating current (ac) field for the purpose of demagnetizing magnetic recording media, usually tapes or disks. The process involves increasing the ac field gradually from zero to some maximum value and decreasing the field back to zero, leaving a very low residue of magnetic induction on the media.

Derivative Classification. A determination in accordance with approved classification guides, source documents, or other guidance of an authorized original classifier that a document contains classified information.

Glossary (continued)

Derivative Classifier. An individual authorized in writing by appropriate authority to derivatively classify National Security Information, Restricted Data, and Formerly Restricted Data. (See also Derivative Classification and Authorized Classifier.)

DES. See Data Encryption Standard.

Document. Any recorded information regardless of its physical form or characteristics including, but not limited to, the following:

1. All handwritten, printed, or typed matter;
2. All painted, drawn, or engraved matter;
3. All sound, magnetic, or electromechanical recordings;
4. All photographic prints and exposed or developed film or still or motion pictures;
5. Automated data processing input, memory, program, or output information or records such as punch cards, tapes, drums, disks, or visual displays;
6. All optical or laser recordings.

Documentation. A statement of the number of pages of a document, the series designation for the particular set of copies, and the number of each copy within the set, or some other unique identification technique for differentiating between each copy of a document.

Downgrade. To assign a lower classification than that previously assigned.

Eavesdropping. Interception of a conversation by surreptitious means through use of electronic equipment without the consent of one or more of the participants.

Electromagnetic Emanations. Signals transmitted as radiation through the air and through conductors.

Eligible or Eligibility. Both initial eligibility and continued eligibility of an individual for access authorization and/or employment clearance, unescorted access to nuclear power facilities, access to unclassified Safeguards Information (SGI), or access to sensitive NRC automated information systems and data.

Glossary (continued)

Emanation. Unintended signals or noise appearing external to an equipment.

Emission Security (EMSEC). That component of communications security (COMSEC) that results from all measures taken to deny unauthorized persons information of value that might be derived from intercept and analysis of compromising emanations from crypto-equipment, information processing systems, and telecommunications systems.

Employment Clearance. An administrative determination that an individual (including a consultant) who is an NRC employee or an applicant for NRC employment and other persons designated by the Executive Director for Operations of the NRC are eligible for employment or continued employment pursuant to Subsection 145b. of the Atomic Energy Act of 1954, as amended.

EMSEC. Emission or emanation security.

Encode. To convert plain text into unintelligible form by means of a code system.

Encrypt. To convert plain text into unintelligible form by means of a cryptosystem.

Facility. An educational institution, manufacturing plant, laboratory, office, building or portion thereof used by NRC or its contractors, or others associated with the NRC program, or by any other organization that is part of or associated with the United States Government.

Facility Approval. A determination by the NRC that classified information is approved to be used, processed, stored, reproduced, transmitted, or otherwise handled at a specific facility.

Facility Register. An index of security facilities.

File Protection. The aggregate of all processes and procedures established in a system and designed to inhibit unauthorized access, contamination, or elimination of a file.

Foreign Assignee. An employee of a foreign regulatory agency who is assigned to the NRC staff for a period of 6 months or more.

Glossary (continued)

Foreign Government Information. Information provided by a foreign government or governments, an international organization of governments, or any element thereof, with the expectation, expressed or implied, that the information, the source of the information, or both, are to be held in confidence. Also, information produced by the United States pursuant to or as a result of a joint arrangement with a foreign government or governments, or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence.

Foreign Intelligence Information (FII). Information relating to the capabilities, intentions, and activities of foreign powers, organizations, or persons, but not including counterintelligence, except for information on international terrorist activities.

Foreign National. All persons who are not citizens of, nationals of, or immigrant aliens to the United States.

Formerly Restricted Data (FRD). Classified information that the Atomic Energy Commission, the Energy Research and Development Administration, or the Department of Energy removed from the Restricted Data category after that agency and the Department of Defense jointly determined that the information relates primarily to the military utilization of atomic weapons and can be adequately safeguarded as National Security Information, subject to the restrictions on transmission to other countries and regional defense organizations that apply to Restricted Data.

Fortuitous Conductor. Any conductor that may provide an unintended path for signals. Fortuitous conductors include cables, wires, pipes, conduits, and structural metal work in the vicinity of a radiation source.

FSTS. Federal secure telephone service.

Guard. A uniformed individual who is employed for and charged with the protection of classified information and/or U.S. Government property.

Glossary (continued)

Handshaking Procedures. A dialogue between a user and a computer, a computer and another computer, or a program and another program for the purpose of identifying a user and authenticating the user's identity through a sequence of questions and answers based on information either previously stored in the computer or supplied to the computer by the initiator of dialogue. Synonymous with password dialogue.

Hardware Security Measures. Equipment features or devices used in an ADP system to preclude deliberate or inadvertent unauthorized acquisition, disclosure, manipulation, or modification of data or information, including classified data or information.

Hearing Counsel. An NRC attorney assigned by the General Counsel to prepare and administer hearings in accordance with 10 CFR Part 10, 5 U.S.C. 7532, or Due Process Procedures (Handbook 12.3, Exhibit 11).

Hearing Examiner. A qualified attorney appointed by the Director, Office of Administration, to conduct a hearing in accordance with 10 CFR Part 10, 5 U.S.C. 7532, or Due Process Procedures (Handbook 12.3, Exhibit 11).

Identification, User. The process that enables, generally by the use of unique machine-readable names, recognition of users as identical to those previously described to an ADP system.

Immigrant Alien. One who has entered the United States under an immigrant visa for permanent residence and who may, if the person so desires and meets statutory requirements, become a United States citizen.

Infraction. An act or omission involving failure to comply with NRC security requirements or procedures.

Intelligence Community and Agency or Agencies Within the Intelligence Community. Refers to the following organizations:

1. The Central Intelligence Agency (CIA).
2. The National Security Agency (NSA).
3. The Defense Intelligence Agency (DIA).
4. Offices within the Department of Defense that collect specialized national foreign intelligence through reconnaissance programs.

Glossary (continued)

Intelligence Community and Agency or Agencies Within the Intelligence Community (continued)

5. The Bureau of Intelligence and Research (INR) of the Department of State.
6. The intelligence elements of the Army, the Navy, the Air Force, and the Marine Corps, the Federal Bureau of Investigation (FBI), the Treasury Department, and the Department of Energy.
7. The staff elements of the Director of Central Intelligence.

Interim Access Authorization. An authorization to permit an individual access to classified information before receiving the reports of investigation on the character, loyalty, and associations of this individual, based upon a determination by the Commission that this action is clearly consistent with the national interest and will not endanger the common defense and security.

Internal Security Audit (ADP). A security audit conducted by personnel responsible to the management of the organization being audited.

Intrusion Detection System. A security alarm system that uses an ultrasonic, infrared, visible light beam, a door contact, or a vibration-sensitive or other type sensor to detect and signal the entry of unauthorized persons into a protected area.

Inventory, COMSEC.

1. The physical verification of the presence of each item of accountable COMSEC material charged to a COMSEC account.
2. A listing of each item of accountable COMSEC material charged to a COMSEC account.

Inventory Report, COMSEC. A report submitted to the NSA Central Office of Record (COR) with a copy to the NRC agency COMSEC custodian (NRC COR) attesting to the inventory of accountable COMSEC material.

Keying Material. A type of COMSEC aid that supplies either encoding means for manual and auto-manual cryptosystems or cryptovariables for machine cryptosystems.

Glossary (continued)

Keyword. Synonym for password.

"L" Access Authorization. An "L" access authorization is normally based upon a National Agency Check, Inquiries and Credit (NACIC) for Federal employees or a National Agency Check plus Credit (NACC) for non-Federal employees conducted by the Office of Personnel Management. This authorization permits individuals access, on a need-to-know basis, to SECRET and CONFIDENTIAL National Security Information or CONFIDENTIAL Restricted Data not related to broad naval nuclear propulsion program policy or direction (e.g., preliminary safety analysis reports, final safety analysis reports, and amendments thereto).

Limited Official Use (LOU). Designation applied to certain unclassified official information originated by the Department of State in oral or documentary form, which is to be given limited internal distribution by U.S. Government agencies and their contractors.

Limited Protection. A form of short-term COMSEC protection applied to the electromagnetic or acoustic transmission of national security-related information.

Local Area Network (LAN). A nonpublic data communication system within a limited geographical area, designed to allow a number of independent devices to communicate with each other over a common transmission system. (LANs are usually restricted to relatively small geographical areas, such as rooms, buildings, or clusters of buildings.)

LOU. See Limited Official Use.

Marking.

1. The physical act of indicating on classified documents the assigned classification, changes in classification, downgrading and declassification instructions, and any limitations on their use.
2. The physical act of indicating on sensitive unclassified information documents the assigned category, changes in the sensitive unclassified information category, and removal from the sensitive unclassified information category.
3. The physical act of indicating on unclassified documents the fact that they contain unclassified information.

Glossary (continued)

Master Facility Register. A central index maintained by the Division of Security of all security facilities of NRC, NRC contractors, and other organizations and persons associated with the NRC program.

Monitor Sheet. A printed security form, generally placed next to a security container, vault, vault-type room, or secure telephone, that is initialed on a scheduled basis by the person(s) assigned to monitor the security of the unit.

National Security. The national defense or foreign relations of the United States.

National Security Council Information (NSCI). Classified information contained in (1) any document prepared by or intended primarily for use by the National Security Council (NSC), its interagency groups as defined in National Security Decision Directive-2 (NSDD-2), dated January 12, 1982, or its associated committees and groups and (2) deliberations of the NSC or its interagency groups, as defined in NSDD-2, or its associated committees and groups.

National Security Information (NSI). Information that has been determined pursuant to Executive Order 12356 or any predecessor order to require protection against unauthorized disclosure and that is so designated.

National Security-Related Information. Unclassified information related to the national defense or foreign relations of the United States.

Naval Nuclear Propulsion Information. In general, all information, classified or unclassified, concerning the design, arrangement, development, manufacture, testing, operation, administration, training, maintenance, and repair of the propulsion plants of naval nuclear-powered ships, including the associated nuclear support facilities.

Need-to-know. A determination by persons having responsibility for classified or sensitive unclassified information that a proposed recipient's access to such information is necessary in the performance of official, contractual, or licensee duties.

Glossary (continued)

NSCI. See National Security Council Information.

NSI. See National Security Information.

NSTISSC. National Security Telecommunications and Information Systems Security Committee.

Official Use Only (OUO). (Reference Sensitive Information.) Unclassified information in oral or documentary form originated by or furnished to NRC, or originated by or furnished to an NRC contractor, licensee, or applicant, that is authorized to be withheld from public disclosure under the provisions of the Freedom of Information Act and/or the Privacy Act and that requires special handling to ensure that the information receives limited internal distribution only and is not publicly disclosed.

Original Classifier. An individual authorized in writing by appropriate authority to originally classify National Security Information. (See Authorized Classifier.)

OUO. See Official Use Only.

Page Check. A check of the pages contained within an item of accountable COMSEC or TOP SECRET material to ascertain that no pages are missing, duplicated, or defective.

Password. A protected word or a string of characters that identifies or authenticates a user, a specific resource, or an access type.

Physical Security, ADP.

1. Use of locks, guards, badges, and similar administrative measures to control access to the computer and related equipment.
2. Measures required for the protection of the structures housing the computer, related equipment, and their contents from damage by accident, intentional action, fire, or environmental hazards. In regard to communications security, "physical security" is the component of COMSEC that results from all physical measures necessary to safeguard COMSEC material and information from access thereto or observation thereof by unauthorized persons. (See also Administrative Security, ADP Security, Communications Security, Data Security, Teleprocessing Security, and Transmission Security.)

Plain Text. Intelligible text or signals that have meaning and that can be read or acted upon without the application of any decryption.

Glossary (continued)

Proprietary Information. (Reference Sensitive Information.) Trade secrets; privileged or confidential research, development, commercial, or financial information, exempt from mandatory disclosure under 10 CFR Part 2 (Sections 2.740 and 2.790) and under 10 CFR Part 9 (Section 9.5); and other information submitted in confidence to the NRC by a foreign source and determined to be unclassified by the NRC.

Protected Distribution System. See Protected Wireline System.

Protected Information. Sensitive unclassified information designated as Limited Official Use, Proprietary Information, Safeguards Information, Official Use Only, and similar information with other designations assigned by U.S. Government agencies, their contractors, or their licensees.

Protected Wireline System. A wireline or fiber-optics system that includes adequate acoustical, electrical, electromagnetic, and physical safeguards to permit its use for the transmission of unencrypted classified information. Synonymous with protected distribution system.

Protective Packaging. Packaging techniques for keying material that discourage penetration, reveal that a penetration has occurred, or inhibit viewing or copying of keying material before the time it is exposed for use.

"Q" Access Authorization. Normally based upon a single-scope full field background investigation (SSBI) conducted by the Federal Bureau of Investigation, the Office of Personnel Management, or another Government agency that conducts personnel security investigations. This authorization permits individuals to have access, on a need-to-know basis, to TOP SECRET, SECRET, and CONFIDENTIAL Restricted Data, Formerly Restricted Data, and National Security Information.

Raw Intelligence (SCI and Collateral). Intelligence information on which there is little or no processing or evaluation to assess its reliability, factual content, or credibility. Documents containing raw intelligence may or may not identify intelligence sources and methods.

Recovery Procedures. The actions necessary to restore a system's computational capability and data files after a system failure or penetration.

Glossary (continued)

Red. A term applied to wirelines, components, equipment, and systems that handle national security signals, and to areas in which national security signals occur.

Red/Black Concept. The concept that telecommunications circuits, components, equipment, and systems that handle classified plain-language information in electrical signal form (Red) be separated from those that handle encrypted or unclassified information (Black).

Registered Initials. One of the elements in an identification technique for restricting access to a computer database or terminal to the individual whose initials have been recorded (registered) with the computer software that restricts access.

Remanence. The residual magnetism that remains on magnetic storage media after degaussing.

Removable Mass Storage Media. Media, including magnetic tapes and disc packs, on which data or information can be entered, held, and retrieved, and that are easily and quickly removed from ADP equipment.

Residue. Data left in storage after processing operations and before degaussing or rewriting.

Restricted Data (RD). All data concerning design, manufacture, or utilization of atomic weapons, the production of special nuclear material, or the use of special nuclear material in the production of energy, but not including data declassified or removed from the Restricted Data category pursuant to Section 142 of the Atomic Energy Act of 1954, as amended.

Risk Analysis. An analysis of systems assets and vulnerabilities to establish estimated expected losses based on the occurrence of adverse events (e.g., fire, power loss, or theft) and the probability of the occurrence of these events.

Sanitizing (ADP). The degaussing or overwriting of sensitive information in magnetic or other storage media. Synonymous with scrubbing.

Scavenging. Searching through residue for the purpose of unauthorized data acquisition.

Glossary (continued)

SCI. See Sensitive Compartmented Information.

SECRET. The classification level applied to information the unauthorized disclosure of which could reasonably be expected to cause serious damage to the national security. (The classification level between CONFIDENTIAL and TOP SECRET.)

Secure Operating System. An operating system that effectively controls hardware and software functions in order to provide the level of protection appropriate to the value of the data and resources managed by the operating system.

Secure Telecommunications Facility. A telecommunications facility that employs crypto-material to protect the transmission of national security information.

Security Area. A physically defined space containing classified information and subject to physical protection and personnel access controls.

Security Assurance. A written certification by which a specifically authorized official of a foreign government or an international organization with which the United States has an international agreement covering the exchange of classified information informs the United States Government of the category of a security clearance held by a foreign national, the scope of the investigation upon which the clearance determination is based, and personal identity data.

Security Clearance (NRC). See Access Authorization.

Security Data (ADP). A term applied to data about protective measures intended to eliminate or reduce threats and vulnerabilities.

Security Facility. Any facility that has been approved by the NRC or another Government agency for using, processing, storing, reproducing, transmitting, or otherwise handling classified information.

Security Facility Approval. See Facility Approval.

Glossary (continued)

Security Importance Rating. An alphabetical letter designating the relative importance to the national security of an activity that involves classified information. These ratings are assigned to security facilities and to individual classified interests within security facilities, as set forth in Management Directive 12.1.

Security Perimeter. See Control Zone.

Security Plan. A document prepared by an NRC office, division, or region, or by a contractor, a consultant, a licensee, or a licensee-related organization describing the organization's or the individual's procedures and measures for safeguarding classified and/or sensitive unclassified interests and for the security education of the employees. This term includes security plans for foreign assignees.

Security Proposal, System. A document that outlines a system, for example, a telecommunications and/or an automated data processing system, and the security measures to protect sensitive or classified information processed, produced, or communicated by the system. Once approved, the proposal becomes a plan.

Security Survey. An onsite examination by an NRC security representative of a security facility to assess the devices, equipment, and procedures employed within an organization or facility to safeguard classified and/or sensitive unclassified information and to protect personnel and property.

Sensitive Application. An automated systems application that requires a degree of protection because it processes sensitive data.

Sensitive Compartmented Information (SCI). All information and materials requiring special community controls indicating restricted handling within present and future community intelligence collection programs and their end products. These special community controls are formal systems of sources and methods and analytical procedures of foreign intelligence programs. The term does not include Restricted Data as defined in Section 11, Public Law 585, Atomic Energy Act of 1954, as amended (42 U.S.C. 2014).

Glossary (continued)

Sensitive Information. That data that requires a degree of protection because of the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the data. This term includes Proprietary Information, unclassified Safeguards Information, naval nuclear propulsion information, and other information withheld from public dissemination under the Freedom of Information Act, the Privacy Act, or the Atomic Energy Act and information not exported to foreign countries or that must not be disclosed to foreign countries. It also includes sensitive unpublished and otherwise unavailable fuel cycle information relating to the technology of enrichment or reprocessing.

Sensitive data falls into the following categories. The examples cited below are illustrative and not all-inclusive. Final determination of the specific data that is sensitive is made by the office director responsible for the data.

Category A – Personal Data: Sensitive or private data related to personnel, medical files, and similar files whose unauthorized disclosure would constitute an unwarranted invasion of privacy. Data types in this category are protected from mandatory public disclosure by 10 CFR 9.5(a)(6). Specific examples of records in this category may include—

1. Files containing the names, personal identifiers, or other identifying data on individuals who have been exposed to radiation.
2. Files or records pertaining to individuals in which disciplinary or administrative actions are documented.
3. Performance appraisal data or data concerning individual qualifications for promotions.

Category B – Financial, Commercial, and Confidential Business (Proprietary) Information: Sensitive data related to financial information and applications, commercial information received in confidence, Proprietary Information, or trade secrets. In addition, this category includes financially related applications, such as automated and equipment inventory systems. Data types in this category are described in 10 CFR 9.5(a)(4). Specific examples of data in this category may include—

Glossary (continued)

Category B – Financial, Commercial, and Confidential Business (Proprietary) Information (continued)

1. Payroll systems.
2. General accounting systems.
3. Automated procurement systems.
4. Inventory control systems.
5. Some contract performance information.
6. Information furnished to the NRC pursuant to a claim that it is proprietary (e.g., foreign or domestic).
7. Information of the type specified in 10 CFR 2.790(d) (e.g., special nuclear material (SNM) control and accounting, the licensee's fundamental nuclear material control plan, and process monitoring).

Category C – Internal Data: Sensitive data related to the internal operations of the NRC. Included in this category are the predecisional versions of internal personnel rules, advance information, and procurement actions. These types of data are further explained in 10 CFR 9.5(a)(2) and 9.5(a)(5). Specific examples of data in this category may include—

1. Methods, findings, and recommendations concerning internal surveys and audits before their publication or other public release.
2. Calculations supporting proposed obligations for specific procurements of goods or services by contract.

Category D – Investigatory, Intelligence, and Security Data: Sensitive data related to investigations for compliance purposes, intelligence-related information that cannot be classified but is protected from public disclosure by statute and system-specific security countermeasures for sensitive activities, and unclassified Safeguards Information (SGI).

These data types include those specified in 10 CFR 9.5(a)(3), 10 CFR 9.5 (a)(7), and Management Directive 12.6. Specific examples of data in this category may include—

Glossary (continued)

Category D – Investigatory, Intelligence, and Security Data (continued)

1. Office of the Inspector General (OIG) investigations.

2. Facility-specific data extracted from Security Survey Reports (NRC Form 140A).

3. **Unclassified Safeguards Information:** Data and information discussing specific protection techniques and their expected levels of deterrence or effectiveness, usually found in facility-specific documents (Management Directive 12.6).

Category E – Other Sensitive Data: Data deemed sensitive by other Federal agencies must be protected by NRC when such data are in NRC's custody. Specific examples of data in this category may include—

1. Data related to the regulation and supervision of financial institutions (5 U.S.C. 552(b)(8)). This information is protected from mandatory public disclosure by 10 CFR 9.5(a)(8).

2. Production data and other data that would yield unfair competitive advantage related to oil wells, sub-surface mining, or drilling locations provided to NRC during consideration of nuclear facility siting (10 CFR 9.5(a)(9)).

3. **Limited Official Use (LOU) Data.** Certain unclassified official information in oral or documentary form originated by the Department of State that is to be given limited internal distribution by U.S. Government agencies and their contractors.

4. **Naval Nuclear Propulsion Information.** Certain unclassified information concerning the design, arrangement, development, manufacture, testing, operation, administration, training, maintenance, and repair of the propulsion plants of naval nuclear power ships, including the associated nuclear support facilities.

Sensitive Unclassified Information. See Sensitive Information.

Approved: November 6, 1992
(Revised: July 15, 1994)

Glossary (continued)

Shared Logic. In word processing, an arrangement in which two or more proximate work stations share common facilities.

Shared Logic Word Processing Equipment. Word processing equipment in which the resources for a processing unit and storage devices are shared between two or more work stations.

Shielded Enclosure. An area (room or container) specifically designed to attenuate electromagnetic radiation or acoustic emanations originating either inside or outside the area.

Significant Information of Intelligence Value. Information useful to a foreign country or to a terrorist preparing or executing an operational plan that is contrary to the best interests of the United States.

Software Security Measures. Computer programs and routines used in an ADP shared logic system to preclude deliberate or inadvertent unauthorized acquisition, disclosure, manipulation, or modification of data or information, including classified data or information.

Source Document. A document, other than a classification guide, from which classified information is extracted and that is used as the basis for the classification of a new document.

Staging. The moving of data from an offline or low-priority device back to an online or higher priority device, usually on demand of the system or on request of the user.

Stand-alone System. A system that requires no other piece of equipment with it to complete its own operation. It can, and usually does, operate independently, for example, a personal computer or a word processor.

Storage Medium. Any device or recording medium into which data can be stored and held until some later time and from which the entire original data can be obtained.

Surreptitious Listening Device. Apparatus or equipment used to obtain information without the knowledge of all persons involved.

Glossary (continued)

System Integrity Study. An examination and analysis of the security measures of an ADP system to determine whether or not any deliberate attempt by personnel or failure of system components could adversely affect the common defense and security.

System Security Officer, ADP. An individual who is knowledgeable in security concepts and principles, including ADP, and technical security concepts and principles and is responsible for the security of one or more systems or facilities.

Technical Surveillance Countermeasures (TSCM) Inspection. Technical inspection of a facility or premises to determine the actual or possible presence of wiretapping or eavesdropping devices. Synonymous with audio countermeasures.

Technological Attack. An attack that can be perpetrated by circumventing or nullifying hardware and software access control mechanisms rather than by subverting system personnel or other users.

Telecommunications. The transmission, communication, or processing of information, including the preparation of such information therefor by electrical, electromagnetic, electromechanical, or electro-optical means.

Telecommunications Protection. The protection resulting from all measures designed to prevent deliberate or inadvertent unauthorized disclosure, acquisition, manipulation, or modification of information in a teleprocessing system. (See also Teleprocessing Security.)

Telecommunications System Security Proposal. A document that outlines a telecommunications system and the security measures to protect sensitive or classified information communicated by the system. Once approved, the proposal becomes a plan.

Teleprocessing. Pertaining to an information transmission system that combines telecommunications, ADP systems, and man-machine interface equipment for the purpose of interacting and functioning as an integrated whole.

Glossary (continued)

Teleprocessing Security. The protection resulting from all measures designed to prevent deliberate, inadvertent, or unauthorized disclosure, acquisition, manipulation, or modification of information in a teleprocessing system. (See also ADP Security, Data Security, Communications Security, Transmission Security, and Telecommunications Protection.)

TEMPEST. A short name referring to investigations and studies of compromising emanations. It is often used synonymously for the term "compromising emanations," for example, TEMPEST tests, TEMPEST inspections.

TEMPEST-Approved Equipment or Systems. Equipment or systems that have been certified with the requirements of the effective edition of NACSIM 5100, TEMPEST Specifications.

TEMPEST Test. A laboratory or onsite (field) test to determine the nature and amplitude of conducted or radiated signals containing compromising information.

Terminal Identification. The means used to establish the unique identification of a terminal by a system.

Third Agency Document. A document originated by personnel of a Government agency or its contractors, by a foreign government, or by an international organization, which was provided to NRC by an organization other than the originator.

Threat Monitoring. The analysis, assessment, and review of audit trails and other data collected for the purpose of searching out system events that may constitute violations or may precipitate incidents involving data privacy matters.

Time-Dependent Password. A password that is valid only at a certain time of the day or during a specified interval of time.

Time-Shared System. A system in which available central computer time is shared among several jobs as directed by a scheduling plan or formula.

TOP SECRET. The classification level applied to information the unauthorized disclosure of which could reasonably be expected to cause exceptionally grave damage to the national security. (The highest classification level.)

Glossary (continued)

Traffic. Messages or voice communications or messages transmitted or received via telecommunications.

Transaction, ADP. A collection or grouping of several related actions entered by a terminal operator that produces a predefined output.

Transmission Security (TRANSEC). The component of communications security that results from all measures designed to protect transmissions from interception and exploitation by means other than cryptanalysis. (See also ADP Security, Data Security, Communications Security, and Teleprocessing Security.)

TSCM. See Technical Surveillance Countermeasures.

TSEC. The abbreviation for telecommunications security. When affixed to a short title, for example, KAM-211A/TSEC, TSEC/KG-52, it indicates material is produced or authorized by the National Security Agency.

Unclassified Safeguards Information (SGI). (Reference Sensitive Information.) Sensitive unclassified information that specifically identifies the detailed security measures of a licensee or an applicant for the physical protection of special nuclear material; or security measures for the physical protection and location of certain plant equipment vital to the safety of production or utilization facilities. Protection of this information is required pursuant to Section 147 of the Atomic Energy Act of 1954, as amended.

Upgrade. To raise the classification level of information.

User Identity Code, ADP. A protected word or a string of characters that identifies or authenticates a user, a specific resource, or an access type.

Validation. The performance of tests and evaluations in order to determine compliance with security specifications and requirements.

Vault. A windowless enclosure constructed with walls, floor, roof, and door(s) that will delay penetration sufficient to permit the arrival of emergency response forces capable of preventing theft, diversion, damage, or compromise of the classified information.

Approved: November 6, 1992
(Revised: July 15, 1994)

Glossary (continued)

Vault-Type Room. A room that has a combination door lock and is protected by an intrusion alarm system that alarms upon unauthorized penetration.

Violations (of laws). Criminal violations of statutes of security interest.

Vulnerability. Characteristics of a friendly telecommunications system or cryptosystem that are potentially exploitable by hostile intelligence entities.

Vulnerability Assessment. The systematic examination of telecommunications to determine the adequacy of COMSEC measures, to identify COMSEC deficiencies, to provide data from which to predict the effectiveness of proposed COMSEC measures, and to confirm the adequacy of such measures after implementation.

Watchman. A person, unarmed and not necessarily uniformed, who provides protection for classified information and/or U.S. Government property.

Weapons Data. Classified information concerning the design, manufacture, or utilization (including theory, development, storage, characteristics, performance, and effects) of atomic weapons or components thereof, including such information incorporated in or relating to nuclear explosive devices.

Wide Area Network (WAN). A network that provides data communication capabilities in geographic areas larger than those served by local area networks (LANs).

Wiretapping. The direct or inductive coupling by surreptitious means of an electronic device to lines transmitting communications without the consent of any of the participants.

Wiretapping or Eavesdropping Devices. Electronic devices designed primarily to surreptitiously intercept communications without the consent of any of the participants.

Working Variable. A cryptovariable distributed by a key generation facility for use on a specific interstation call.

Zeroize. To remove or eliminate the cryptovariable from a crypto-equipment or fill device.