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'
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.

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

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

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, 5U.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, 5U.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.

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 dorr(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.

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.

TN: DT–00–19

To: NRC Management Directives Custodians

Subject: Transmittal of Directive 12.1, "NRC Facility Security Program"

Purpose: Directive and Handbook 12.1 have been revised for clarity and to reflect organizational changes within NRC. Changes were made to the responsibilities and authorities portion of the directive to: (1) include the IG responsibility to authorize OIG criminal investigators to carry firearms; and (2) reflect the respective jurisdictions of the Office of the Inspector General and the Office of Investigations. Several revisions in the handbook were made to comply with changes as a result of Executive Orders 12829, "National Industrial Security Program," and 12958, "Classified National Security Information." Additional changes to the handbook have been made to reflect more accurately operations and procedures associated with the NRC facilities security program.

Office and Division of Origin: Office of Administration

Contact: Cindy G. Harbaugh, (301) 415–7050

Date Approved: April 28, 1993 (**Revised: October 16, 2000)**

Volume: 12 Security

Part: 1

Directive: 12.1 NRC Facility Security Program

Availability: Rules and Directives Branch
Office of Administration
David L. Meyer (301) 415–7162 or
Doris Mendiola (301) 415–6297

NRC Facility Security Program

Directive 12.1

Contents

Policy 1

Objectives 1

Organizational Responsibilities and Delegations of Authority 1

General Counsel. Office of the General Counsel (OGC) 1
Executive Director for Operations (EDO) 2
Deputy Executive Director for Management Services (DEDM) 2
Director. Office of Administration (ADM) 2
Director. Office of Investigations (O1) 2
Office Directors and Regional Administrators 3
Director. Division of Facilities and Security (DFS). ADM 4

Applicability 4

Handbook 4

References 4

NRC Facility Security Program Directive 12.1

Policy
(12.1–01)

It is the policy of the **U.S.** Nuclear Regulatory Commission to provide physical security requirements and procedures to protect classified information, sensitive unclassified information, and facilities and NRC assets. This directive and handbook do not affect Commission rules and regulations applicable to NRC licensees that are contained in the ***Code*** of ***Federal Regulations.***

Objectives
(12.1–02)

- To ensure that classified and sensitive unclassified information is protected from unauthorized disclosure under pertinent laws, Executive orders, management directives, and applicable directives of other Federal agencies and organizations. (021)
- To ensure that NRC assets are protected from damage or loss to the greatest extent possible. (022)

Organizational Responsibilities and Delegations of Authority
(12.1–03)

General Counsel, Office of the General Counsel (OGC)
(031)

Performs legal review of facility security-relatedmatters and concurs in the EDO decision to authorize and conduct any monitoring or recording of conversations.

Inspector General, Office of the Inspector General (OIG)

(032)

- Provides DFS any information developed or received relating to security matters. (a)
- Authorizes carrying of firearms by OIG criminal investigators (special agents). If designated and sworn as Special Deputy United States Marshals, special agents of the OIG are authorized to carry firearms by 18 U.S.C. Section 3053 as directed by the IG and in accordance with the IG Act, 5 U.S.C. App. 3, and Chapter **6,** OIG "Special Agents Handbook." (b)
- Approves the surreptitious use of electronic, mechanical, or other devices for monitoring, recording, or intercepting conversations, as authorized by law. (c)

Executive Director for Operations (EDO)

(033)

Approves the use of devices covered by Handbook 12.1, Part **VI,** for monitoring or recording conversations, as authorized by law.

Deputy Executive Director for Management Services (DEDM)

(034)

Ensures that the NRC Facility Security Program is operated in an efficient and effective manner consistent with existing policies, regulations, and in a manner that protects against identified threats.

Director, Office of Administration (ADM)

(035)

Oversees the NRC Facility Security Program as carried out by the NRC Division of Facilities and Security (DFS).

Director, Office of Investigations (OI)

(036)

Provides DFS any information developed or received relating to security responsibilities in accordance with the OI/SEC agreement of February 1983.

Office Directors and Regional Administrators
(037)

- Ensure that NRC employees and NRC contractor personnel under their jurisdiction are cognizant of and comply with the provisions of this directive and handbook, as appropriate. (a)
- Advise DFS of the existence or proposed creation of any business relationship or interest that would require DFS's review of any contract, subcontract, or similar action and of any significant change or termination of any classified or sensitive unclassified interests in organizations and functions under their jurisdiction. (b)
- Furnish security plans to DFS for review or approval, as appropriate. (c)
- Advise DFS of any information that indicates noncompliance with this directive and handbook or that is otherwise pertinent to the proper protection of classified interests, sensitive unclassified information, or NRC assets. (d)
- Take or direct action, as requested by DFS, or as otherwise may be pertinent, regarding deficiencies in security or property protection in facilities or functions under their jurisdiction. (e)
- Support and implement the NRC Security Education/Awareness Program for personnel under their jurisdiction, including ensuring that subordinate NRC supervisors discharge their responsibility for on-the-job security education/awareness of their employees. ***(f)***
- Support and implement the NRC Security Infraction Program in all organizations and functions under their jurisdiction, including submitting infraction reports to DFS. (g)
- Control and safeguard classified and sensitive unclassified information under their jurisdiction in accordance with this directive and handbook. (h)
- Request exceptions to or deviations from this directive and handbook, as required. (i)

Director, Division of Facilities and Security (DFS), ADM
(038)

- Plans, develops, establishes, and administers policies, standards, and procedures for the overall NRC Facility Security Program, including the approval of facilities for the handling and storage of classified and sensitive unclassified information. (a)
- Administers the NRC Security Education/Awareness Program. (b)
- Administers the NRC Security Infraction Program and coordinates action, as appropriate, with other NRC and Federal organizations regarding incidents of possible disclosure of classified information or other violations of Federal law or statutes. (c)

Applicability
(12.1–**04)**

The policy and guidance in this directive and handbook apply to all NRC employees and to all NRC contractors to whom they apply as a condition of a contract or purchase order.

Handbook
(12.1–*05)*

Handbook 12.1 contains guidelines and procedures with regard to facility security, the protection of classified information and facilities, the safeguarding of NRC property and programs, and the administration of the NRC security awareness program and security infraction program.

References
(12.1–06)

Atomic Energy Act of **1954,** as amended **(42** U.S.C. 2011 et seq.).

Code of *Federal Regulations*—

10 CFR Part 25, "Access Authorization for Licensee Personnel."

10 CFR Part 95, "Facility Security Clearance and Safeguarding of National Security Information and Restricted Data."

10 CFR Part 160, "Trespassing on Commission Property."

41 CFR 101-120.5, "Federal Property Management Regulations.''

References

(12.1–06) (continued)

Coordination of Counterintelligence Activities (50 U.S.C. 402a, Sect. 811)

Crimes and Criminal Proceedings (18 U.S.C.).

Directive 1/21, "Physical Security Standards for Sensitive Compartmented Information Facilities (SCIF)," Director of Central Intelligence, July 29, 1994.

Energy Reorganization Act of 1974, as amended (42 U.S.C. 5801 et seq.).

Executive Order 10865, as amended, "Safeguarding Classified Information Within Industry" (February 20, 1960).

— 12829, "National Industrial Security Program" (NISP), January 6, 1993.

— 12958, "Classified National Security Information" (April 17, 1995), and related Information Security Oversight Office directives.

— 12968, "Access to Classified Information," August 2, 1995.

Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.).

Freedom of Information Act (5 U.S.C. 552).

Inspector General Act of 1978 (5 U.S.C., App. 3)

NISP Operating Manual (NISPOM), Department of Defense 5220.22M, January 1995, and Supplement 1, February 1995.

NRC Management Directive—

2.3, "Telecommunications."

3.1, "Freedom of Information Act."

3.2, "Privacy Act."

11.1, "NRC Acquisition of Supplies and Services."

11.7, "NRC Procedures for Placement and Monitoring of Work With the U.S. Department of Energy (DOE)."

12.2, "NRC Classified Information Security Program."

References

(12.1–06) (continued)

12.3, "NRC Personnel Security Program."

NRC, OIG, "Special Agents Handbook."

NRC, "OI/SEC Agreement of February 1983."

Omnibus Crime Control and Safe Streets Act of 1968, Title 111, "Wire Interception and Interception of Oral Communications" (18 U.S.C. 2510 et seq.).

Privacy Act of 1974, as amended (5 U.S.C. 552a and App. 3).

Security Policy Board, Executive Branch, "Directive on Safeguarding Classified National Security Information," draft February 28, 1995.

—, Provisions of the NISP, September 19,1996.

U.S. Department of Defense and U.S. Nuclear Regulatory Commission Memorandum of Understanding, concerning the NISP, April 2, 1996.

NRC Facility Security Program

Handbook 12.1

Contents

Part I

Facility Clearance and Surveys 1

Establishment of Security Facilities (A) 1
Basic Considerations (1) 1
Notification of Classified Interests (2) 2
The Facility Clearance Process (B) 2
NRC. NRC Contractor. and NRC Consultant Facilities (1) 2
Special Requirements for the Department of Energy (DOE) National Laboratories (2) 3
Special Requirements for Industrial Facilities at Which NRC and DOE Have Interests (3) 3
Facilities of the Department of Defense (DOD). DOD Contractors. and DOD Consultants (4) 4
Other Federal Agencies (Excluding DOD Facilities) and Their Contractors or Consultants (5) 5
Continuing Facility Clearance (C) 5
NRC. NRC Contractor. and NRC Consultant Facilities (1) 5
DOE National Laboratories (2) 6
DOD. DOD Contractor. and DOD Consultant Facilities (3) 6
Other Federal Agencies (Excluding DOD Facilities) and Their Contractors and Consultants (4) 6
Terminating Facility Clearance (D) 7
Special Considerations Applicable to Bidders (E) 7
Security Surveys(F) 8
Basic Considerations (1) 8
Coverage (2) 8
Reporting (3) 9
Physical Protection Facilities (G) 10
Notification (1) 10
Physical Protection Surveys (2) 10
Facility Data Reports and the Master Facility Register (H) 10
Facility Data Reports (1) 10
Master Facility Register (2) 11

Contents (continued)

Part II

Physical Security Requirements for the Protection of Classified Information 12

Overview of Physical Security (A) 12
Basic Considerations (1) 12
Access Controls and Authorization (2) 13
Control of Areas (3) 13
Package Inspection (4) 14
Personnel and Vehicular Access Controls (5) 15
Personnel Identification System (B) 16
NRC Permanent Identification Badge (1) 16
NRC Visitor Badges (2) 16
Temporary Badges for Employees (3) 17
Records (4) 17
Lost Badges or Passes(5) 18
Recovery (6) 18
Reissuance of Badges or Passes (7) 18
Special Requirements for Security Areas (8) 18
Physical Barriers (C) 18
Intrusion Detection (D) 20
Interior Protective Alarms (1) 20
Protective Lighting (2) 21
Protective Personnel (E) 21
Guard Force 21
Protection of Classified Information in Use (F) 22
Requirements (1) 22
Destruction of Classified Information (2) 23
Classified Conferences (3) 23
Prevention of the Use of Surreptitious Listening Devices (4) 24
Photocopy Machine Control *(5)* 25
Storage of Classified Information (G) 25
Security Containers (1) 26
Requirements for Storage (2) 27

Contents (continued)

Part II (continued)

Alternate Storage Locations (3) 29
Miscellaneous Storage Specifications and Procedures (4) 29
Trespassing on Commission Property (H) 32
Statutory Provisions (1) 32
Criteria (2) 32
Proposals (3) 32
Posting Requirements (4) 33
Notification of the Federal Bureau of Investigation (5) 34
Violations (6) 34

Part III

Protection of Unclassified NRC Facilities 35

Criteria (A) 35
Guidance (B) 36
General (1) 36
Standards and Requirements (2) 36
Occupant Emergency Program (C) 38
Occupant Emergency Plan (1) 38
Designated Official (2) 39
Non-Federal Facility Emergency Plan (D) 39

Part IV

Security Awareness 40

Program Design (A) 40
Program Components (B) 41
Security Orientation Briefing for New Employees (1) 41
Briefing on Safeguarding Classified Information (2) 41
Continuing Refresher or Special Security Awareness Efforts (3) 42
Briefing on Termination of Access (4) 43
Program Records (C) 43

Contents (continued)

Part V

Infractions and Violations 45

Infractions (A) 45
Security Infraction (1) 45
Administrative Action (2) 45
Reporting Infractions (3) 48
Preliminary Inquiry (4) 49
Violations (B) 50
Violation (1) 50
Handling a Violation (2) 50
Reporting Procedures (3) 50
Content of Report (4) 51
Investigation of Violations (5) 52
Assistance to Federal Law Enforcement Agencies (6) 52
Followup of Alleged or Suspected Violations of Security (7) 52
Losses or Compromise of Classified Information or Sensitive Unclassified Information (C) 52
Reporting Procedures (1) 52
Content of Report (2) 53
Action (3) 53
Damage Assessment (4) 54
Records Maintained (5) 56
Actions Against Individuals (6) 56

Part VI

Prohibitions on Wiretapping and Eavesdropping Devices 58

Procurement and Use of Devices (A) 58
Services Available From the Division of Facilities and Security (B) 58
Technical Inspection (1) 58
Notification (2) 59
Staff Assistance (3) 59
Actions To Be Taken Upon Discovery of Devices (C) 59
By Individuals (1) 59

Contents (continued)

Part VI (continued)

By DFS (2) 60
Classification (3) 60
Advance Notice of Attachment of Any Devices to Telephone or Teletype Lines (D) 60
EDO Approval (1) 60
Line Compatibility (2) 61
Instructions to NRC and Contractor Personnel (E) 61

Exhibits

1 Certificate of Possession 62
2 Certificate of Non-Possession 63
3 Standard Form 700. "Security Container Information" 64
4 Standard Form 702. "Security Container Check Sheet" 65
5 Standard Form 312. "Classified Information Nondisclosure Agreement" 66

Part I

Facility Clearance and Surveys

This part provides procedures for granting and terminating NRC clearances for security facilities, designating and terminating physical protection facilities, and surveying these facilities to ensure compliance with established security standards.

Establishment of Security Facilities (A)

Basic Considerations (1)

A security facility is any facility that has been cleared by NRC to use, process, store, reproduce, transmit, or otherwise handle NRC classified information. Security facilities are established to provide a standardized program of protection for classified information at the locations involved. (a)

Facility clearance is the process by which NRC determines that a facility is eligible to handle NRC classified information. The Division of Facilities and Security (DFS), Office of Administration, surveys these facilities to evaluate the adequacy of the security protection afforded NRC classified information. NRC facility clearance is granted at a level commensurate with the anticipated level of NRC classified information to be received, stored, or otherwise handled by the facility. (b)

In certain instances, DFS bases facility clearance on assurances from another Federal agency that it has similar security measures in place. In these instances, the facility must be under the active direction of that agency's security program, and DFS must be provided assurance that NRC classified information will be afforded protection in accordance with acceptable security criteria, such as Executive Order 12958. (c)

Establishment of Security Facilities (A) (continued)

Notification of Classified Interests (2)

All NRC offices and divisions must promptly notify DFS of their intent to initiate any classified contract, subcontract, or similar interest under their jurisdiction or sponsorship. A completed NRC Form 187, "Security/Classification Requirements," and a statement of work must be submitted to DFS. On the basis of this submission, DFS will initiate necessary actions to confirm an existing facility security clearance or establish such a clearance for the facility. (a)

An existing facility clearance may be used provided the approval for classified information is at the same or lower classification level and the proposed security interest may be included. The responsible NRC office also will notify DFS of any significant change in or termination of a classified interest previously reported. Additional information and guidance concerning contract administration can be found in Management Directive (MD) 11.1, "NRC Acquisition of Supplies and Services." (b)

The Facility Clearance Process (B)

NRC, NRC Contractor, and NRC Consultant Facilities (1)

The basis for facility clearance is: a favorable foreign ownership, control or influence (FOCI) determination (reference Handbook 12.2, "NRC Classified Information Security Program," Part I(F)); a satisfactory security survey rating; an appropriate number of personnel access authorizations; and a DFS-approved facility security plan. The security plan must be prepared and the security survey must be conducted no more than 6 months before the facility clearance is granted. If more than 6 months has elapsed, DFS will conduct a special survey or otherwise ensure that the conditions and procedures described in the security survey report and the security plan are still in effect. (a)

Although the nature of a security plan dictates that each plan be somewhat unique, all security plans must contain a written statement originated by the appropriate NRC office, division, region, contractor, consultant, or other interest describing the organization's procedures and measures for safeguarding NRC classified information and for ensuring that employees receive security education. As a rule, the

The Facility Clearance Process (B) (continued)

NRC, NRC Contractor, and NRC Consultant Facilities (1) (continued)

requirements contained in this directive will be used in formulating the security plan. DFS may be consulted at any time for advice and assistance to develop the required security plan and normally provides this assistance as a matter of course during the facility clearance process. (b)

In special instances, DFS may grant an interim facility clearance before an initial security survey is conducted. Interim facility clearance will be based on a favorable FOCI determination, an appropriate number of NRC access authorizations, a DFS-approved facility security plan. Thereafter, the initial security survey will be conducted as soon as practical. As a result of the initial security survey, DFS will grant facility clearance or will continue or terminate the interim facility clearance pending compliance with survey recommendations. (c)

Special Requirements for the Department of Energy (DOE) National Laboratories (2)

DOE work performed for NRC is subject to security requirements other than the provisions of this part. These other requirements are contained in the National Industrial Security Program Operating Manual (NISPOM) dated January 1995, and Supplement 1 dated February 1995. Under the NISPOM, DOE assumes security cognizance for NRC classified interests at DOE national laboratory facilities and provides DFS assurance that adequate security will be afforded NRC classified interests. All NRC offices and divisions must promptly notify DFS of their intent to initiate NRC classified work at DOE national laboratories. (See also MD 11.7, "NRC Procedures for Placement and Monitoring of Work With the U.S. Department of Energy (DOE).")

Special Requirements for Industrial Facilities at Which NRC and DOE Have Interests (3)

For industrial facilities, defined as non-Governmental organizations other than the National Laboratories and the United States Enrichment Corporation, at which both NRC and DOE have authorized either the possession of or access to (nonpossessing facilities) classified information, security requirements other than the provisions of this part are specified in a DOE and NRC Memorandum

The Facility Clearance Process (B) (continued)

Special Requirements for Industrial Facilities at which NRC and DOE have Interests (3) (continued)

of Understanding (MOU), dated September 19, 1996. Under this MOU, NRC and DOE agree to provide mutual security services for the protection of Classified information released to or within industry on behalf of NRC using the specific requirements, restrictions, and other safeguards as prescribed in the National Industrial Security Program Operating Manual (MSPOM) and its supplement.

Facilities of the Department of Defense (DOD), DOD Contractors, and DOD Consultants (4)

Under the MSP, DOD is responsible for the security, as prescribed in the NISPOM and its supplement, of all classified interests at its facilities; therefore, NRC facility clearance is not necessary. (a)

An MOU, dated April 2,1996, between the ***NRC*** and the DOD reflects an agreement that NRC and DOE will provide mutual security services for the protection of classified information released to or within industry on behalf of NRC or DOD. The MOU further states that NRC and DOD will apply the specific requirements, restrictions, and other safeguards as prescribed in the NISPOM and its supplement. (b)

Certain additional security considerations may be required in the following instances: (c)

- ***o*** **Existing DOD Contractor and Consultant Facilities Engaged Directly by NRC or Its Contractors for Work Involving Classified Information.** NRC approval to perform work requiring access to NRC classified information is based on the existing DOD facility clearance (Confidential, Secret, or Top Secret), provided that the DOD facility clearance includes the NRC classified interest. The responsible DOD security office shall furnish DFS **a** copy **of** its security inspection report covering, or otherwise ensuring, the adequate security protection of the NRC classified interest at the facility. The responsible DOD security office must agree that it will notify DFS before its facility clearance is downgraded or terminated. All DOD contractors and consultants having access to NRC classified information must hold comparable DOD access authorizations. If Restricted Data is involved, the mandatory personnel access authorization requirements of the Atomic Energy Act of 1954, as amended, must be followed. (i)

The Facility Clearance Process (B) (continued)

Facilities of the Department of Defense (DOD), DOD Contractors, and DOD Consultants (4) (continued)

- ***Special Considerations.*** If the requirements of Section (B)(4)(c) of this part are not met, or if NRC Top Secret information is involved, DFS shall grant facility clearance in accordance with Section (B)(1) of this part. (ii)

Other Federal Agencies (Excluding DOD Facilities) and Their Contractors or Consultants *(5)*

The basis for NRC facility clearance is formal assurance from the responsible agency official that NRC classified information in its possession or in the possession of its contractors and consultants will be provided appropriate protection. The responsible agency official will provide either a copy of the other agency's security inspection report or similar assurance that documents the adequate security protection of the NRC classified interests at the facility. The mandatory personnel access authorization requirements of the Atomic Energy Act of 1954, as amended, must be followed for access to Restricted Data. (a)

If this assurance cannot be obtained, facility clearance is granted in accordance with the procedures contained in Section (B)(l) of this part. Additionally, if a specific agreement exists between NRC and another Federal agency that limits the dissemination of certain categories of NRC classified information within that agency, DFS will, upon execution of the agreement, request that agency to furnish a statement of its procedures for ensuring the limitation. The responsible Federal agency security office must agree that it will notify DFS before its facility clearance is downgraded or terminated. (b)

Continuing Facility Clearance (C)

At each security facility, DFS assesses compliance with security requirements and the adequacy of procedures to safeguard NRC classified information. This continuing assessment program for each type of facility includes the following:

- **NRC, NRC Contractor, and NRC Consultant Facilities** (1)

  Require a periodic security surveys resulting in a "satisfactory" security rating.

Continuing Facility Clearance (C) (continued)

- **DOE National Laboratories (2)**

  See Section (B)(2)of this part for special requirements.

- **DOD, DOD Contractor, and DOD Consultant Facilities (3)**

  Generally, NRC periodic surveys are not required. However, if an agreement exists between the NRC and DOD (or another Federal agency subject to DOD industrial security services) that specifically limits the dissemination of certain categories of NRC classified information, the responsible security official will submit an annual statement to DFS addressing the effectiveness of the other agency's procedures in meeting this agreement. (a)

  Other security measures may be required for existing DOD contractor and consultant facilities engaged directly by NRC or its contractors for work involving NRC classified information. These security measures require the responsible DOD security office to furnish DFS, on a periodic basis, a copy of its security inspection report, or other assurance of adequate security safeguards, covering the NRC Confidential or Secret interests at the facility. (b)

- **Other Federal Agencies (Excluding DOD Facilities) and Their Contractors and Consultants** (4)

  Normally, periodic surveys are not required, except as specified in Section (C)(4)(b) of this part. However, surveys may be conducted upon request by or agreement with the particular agency involved. Additionally, other security measures may be required in the following instances:

  - **Special Considerations.** If an agreement exists between NRC and the Federal agency to limit the dissemination of certain categories of NRC classified information, the responsible security office must submit an annual statement to DFS regarding the effectiveness of its procedures in meeting this agreement. (a)

  - **Federal Records Centers.** A periodic security survey resulting in a "satisfactory" security rating is required for a Federal Records Center storing NRC classified information. (b)

Terminating Facility Clearance (D)

DFS will terminate the facility clearance when a facility has completed its NRC classified activities or no longer requires NRC classified information. In these cases, DFS will ensure that classified information has been destroyed or returned to appropriate NRC custody. **(1)**

In certain instances, the responsible party may demonstrate a need to retain possession of NRC classified information after the completion or termination of an NRC contract, subcontract, or other agreement. The responsible party shall complete a "Certificate of Possession" (see Exhibit 1), and DFS will conduct periodic security surveys to ensure the continued protection of NRC classified information. (2)

However, when the termination of an NRC classified interest results in the termination of the facility clearance, this process is accomplished by means of a termination survey, by correspondence, or other appropriate means, and includes the actions listed below: (3)

- **Security Termination Statements.** All individuals granted NRC access authorizations who, as a result of the termination of the contract, subcontract, or other agreement, no longer require NRC access authorizations, shall complete and forward to DFS, through the responsible security official, an NRC Form **136,** "Security Termination Statement." (a)

- **Certificate of Nonpossession.** The responsible security official, or other designated official, shall complete and forward to DFS a "Certificate of Nonpossession" (Exhibit 2), which certifies that all NRC classified information associated with the contract, subcontract, or other agreement has been destroyed in accordance with NRC security regulations or has been returned to appropriate NRC custody. (b)

- **Cancellation of Pending Access Authorizations.** The responsible security office shall notify DFS in writing to cancel all pending requests for access authorization under the terminated contract, subcontract, or other agreement. (c)

Special Considerations Applicable to Bidders (E)

Facility clearances for bidders or prospective contractors are granted, continued, or terminated in accordance with Sections (A) through (D) of this part. These clearances may be granted on a short-term basis for a

Special Considerations Applicable to Bidders (E) (continued)

particular procurement action or continued on a standby status to accommodate a current or projected procurement action. (1)

Unsuccessful bidders are required to destroy or return to NRC custody all classified information received or generated in connection with their proposals, as directed by the NRC official issuing the solicitation. This action must be accomplished within 15 days after receipt of notification that a purchase order or a contract has been awarded or that the bid invitation has been withdrawn. *(2)*

Security Surveys (F)

Basic Considerations (1)

A security survey of an NRC facility, internal organizational component, or an NRC contractor facility provides a basis for evaluating the adequacy and effectiveness of the administration of the security program and the protection afforded NRC classified or sensitive unclassified information, employees, and assets. It also thoroughly examines the policies and procedures in effect to ensure compliance with NRC security regulations. These surveys include—

- Initial Security Survey. A survey conducted before facility clearance is granted. (a)
- Periodic Security Survey. A facility or organizational survey conducted at regular or scheduled intervals. (b)
- Special Security Survey. A facility or organizational survey conducted to address specific or immediate problems, questions, or deficiencies and usually performed between periodic surveys or before an initial security survey of the facility. (c)
- Termination Security Survey. A facility survey conducted to ensure the proper termination of NRC security interests. (d)

Coverage (2)

Initial and periodic security surveys examine safeguards afforded all NRC classified interests and include a critical examination of all applicable components and elements of the security program. (a)

Security Surveys (F) (continued)

Coverage *(2)* (continued)

Special security surveys evaluate the adequacy of existing protection for new activities and the need for changes to security procedures as a result of other conditions, such as renovation or remodeling **of** the facility, or new security measures to correct security deficiencies. (b)

Termination security surveys ensure classified interests are terminated and security termination actions are completed. (c)

Reporting (3)

Report of Survey (a)

Following the completion of a security or physical protection survey (see Section (G) of this part), DFS prepares a written report to document the results of the survey. DFS verbally advises the responsible organization of all deficiencies and recommendations upon completion of the survey and in writing following completion **of** the survey report.

Report of Action Taken (b)

Upon receipt of DFS's survey findings, the responsible organization shall inform DFS of those actions taken by the date specified by DFS. When the required action cannot be completed by the prescribed date, the responsible organization will keep DFS informed on the status of the action to be taken.

Immediate Corrective Action (c)

When a security deficiency is discovered during a survey that poses an imminent or serious threat to NRC classified interests, DFS provides immediate onsite direction to correct the deficiency. When such a situation cannot be corrected, DFS takes immediate measures to remove the classified interests and suspend or terminate facility clearance pending corrective action. Similarly, the responsible organization or facility shall immediately notify DFS of any situation or occurrence that poses an imminent or serious threat to NRC classified interests. DFS provides advice and assistance as to any corrective actions to be taken. Similarly, immediate actions will be taken, as appropriate, to address deficiencies that pose an imminent or serious threat to NRC sensitive unclassified interests.

Physical Protection Facilities (G)

Notification (1)

Certain NRC facilities that are not designated "security facilities" must be designated "physical protection facilities" when they are within the scope of the specific security criteria set forth in Part **III** of this handbook. (a)

The responsible NRC office or division shall promptly notify DFS of any facility, contractor or otherwise, that is subject to this protection. This notification must include the name and address of the facility, its function, the nature of the interest, and the name and title of the individual responsible for its protection. (b)

The responsible NRC organization also will notify DFS of any termination or significant change in the interest at any facility previously reported. (c)

Physical Protection Surveys (2)

NRC security representatives conduct the following onsite critical examinations of **a** physical protection facility to ensure safeguarding of property or sensitive NRC interests:

- **Initial Physical Protection Survey.** The first survey conducted after a facility has been designated as a "physical protection facility." (a)
- **Periodic Physical Protection Survey.** A survey conducted subsequent to the initial survey. (b)
- **Special Physical Protection Survey. A** survey conducted to address specific problems, questions, or deficiencies and performed as necessary. (c)
- **Termination Physical Protection Survey.** A survey conducted to confirm the termination of property or sensitive NRC interests. (d)

Facility Data Reports and the Master Facility Register (H)

Facility Data Reports (1)

DFS prepares an original or an amended facility data report (FDR) on the basis of information received from NRC organizations concerning security facilities or physical protection facilities under their jurisdiction.

Facility Data Reports and the Master Facility Register (H)(continued)

Master Facility Register (2)

DFS uses the FDRs to prepare a facility register that indicates the name and address of each facility, whether it is a security facility or a physical protection facility, the nature of the **NRC** interest, the responsible **NRC** contracting office or other office, the name and title of the security or physical protection administrator, the month and year of each survey, and the current survey rating: **"U"** (unsatisfactory) or **"S"** (satisfactory).

Part II

Physical Security Requirements for the Protection of Classified Information

This part provides the practices and procedures for the protection of classified information and facilities pursuant to the Atomic Energy Act of **1954,** as amended; and the Energy Reorganization Act of **1974,** as amended; and Executive orders (e.g., Executive Order 12958).

Overview of Physical Security (A)

Each Federal agency must establish controls to ensure that classified information is used, stored, processed, reproduced, transmitted, and destroyed only under conditions that will provide adequate protection and prevent access by unauthorized persons. Physical security as it relates to the protection afforded classified information is composed of those measures by which physical controls and administrative procedures are used to adequately deter its unauthorized disclosure. The Division of Facilities and Security (DFS), Office of Administration, establishes, maintains, and oversees these controls.

Basic Considerations (1)

The factors to be taken into consideration in determining the type and degree of physical protection to be afforded classified information include —

- The level of the classified information, such as Top Secret, Secret, or Confidential; the relative vulnerability of that information to espionage, sabotage, theft, or other unlawful activity; and the need for compartmentalization of the information. (a)

- The relative importance of the facility, or the information housed in the facility, to the overall NRC program, considering such items as the availability of alternate facilities and information that could be used in an emergency. (b)

Overview of Physical Security (A) (continued)

Basic Considerations (1) (continued)

- The location, size, and arrangement of the facility that houses the classified information and the need to integrate security measures with facility operations. (c)
- The relative efficiency, effectiveness, and economy of alternative methods of protection. (d)

Access Controls and Authorization (2)

Access controls must be established to provide adequate protection and prevent access by unauthorized persons to classified information. (a)

Access to classified information must be limited to persons who possess the appropriate access authorization and who require access to the information in the performance of their official Government duties or contractual obligations. (b)

Persons without appropriate access authorization for the area visited must be escorted at all times by a person possessing the appropriate access authorization while within a security area or any other area in which unsecured classified information is located, such as open storage areas. Additionally, when there are local or unique restrictions on access because of operating, technical, or compartmentalization considerations, only persons knowledgeable of these restrictions shall serve as escorts. Persons without the appropriate access authorization do not require escort within nonsecurity areas or facilities when the classified information located in these areas or facilities is properly secured. (c)

Control of Areas (3)

Physical and administrative controls will be established and maintained to control access by individuals to certain predesignated areas to protect classified information located in these areas.

Security Area (a)

A security area is a physically defined space (usually a room, or a series of interconnecting rooms, within a facility) containing classified information and subject to physical protection and personnel access controls. **A** security area will be established when the nature, size,

Overview of Physical Security (A) (continued)

Control of Areas (3) (continued)

revealing characteristics, sensitivity, or importance of the classified information is such that access cannot otherwise be effectively controlled. Entry into the area must not, in itself, constitute access to classified information.

Controlled Area (b)

A controlled area is a space over which the 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 a lock that provides reasonable protection against surreptitious entry. Entry into a controlled area must not, in itself, constitute access to classified information. DFS determines the nature and degree of the minimum controls necessary to establish and maintain controlled areas.

Package Inspection (4)

Packages, parcels, briefcases, and any other similar containers will be subject to inspection. The purpose of this inspection is to ensure that prohibited articles are not admitted into the facility.

Prohibited Articles (a)

Any article that could result in the illegal or covert compromise of classified or sensitive unclassified information or cause property damage or personal injury is prohibited. Prohibited articles include any camera, copying, recording device, firearm, explosive, incendiary device; or any other item similar in effect or purpose. Only upon request to and approval **of** the Director, DFS, his or her designee, or a regional administrator will an exception be permitted. (i)

Use of NRC-owned recording, photographic, or other equipment in areas other than security areas **issued expressly for** the purpose of accomplishing official NRC business is **not** prohibited or restricted by this requirement. Individuals responsible for such NRC equipment shall take necessary actions to ensure that the equipment is not used in "security areas" or whenever it could knowingly or unknowingly compromise classified or sensitive unclassified information. Similarly, the prohibition on the admittance of a firearm, a two-way radio, or

Overview of Physical Security (A) (continued)

Package Inspection (4) (continued)

similar law enforcement equipment would not normally apply to Federal, State, or local law enforcement authorities whose duties require the possession of these articles. (ii)

Notices (b) .

Written announcements setting forth the policy and requirements regarding prohibited articles will be conspicuously posted at the entrance to the facility or area concerned.

Special Considerations (c)

Notwithstanding the above, packages, briefcases, parcels, and any similar containers of any visitor or employee may be inspected whenever the Director, DFS, or a regional administrator decides that inspection is warranted.

Possible Violations of Law (d)

When inspection of a package, box, briefcase, or similar container discloses a prohibited article and there is no reasonable explanation for its presence, the matter must be reported to the Director, DFS. Similarly, when there is an indication of a possible violation of Federal law, the matter must be reported immediately in accordance with Part V of this handbook.

Personnel and Vehicular Access Controls *(5)*

Positive Identification (a)

Verification of the identity of persons authorized access to NRC security areas, or other areas as determined by DFS, will be accomplished at the designated entry points by a guard, a receptionist, or other person assigned for that purpose, except that remote identification by television may be used, for example, closed circuit television, provided positive identification is ensured.

Entrance Equipment (b)

Entrances to and exits from NRC security areas, or other areas as determined by DFS, may be equipped with metal and/or explosives detectors, doors, gates, rails, or other movable barriers to screen, direct, and control personnel, packages, or vehicles through designated portals.

Personnel Identification System (B)

A pass or badge system will be used to control access to security areas or any other area designated by DFS in which 30 or more people are employed per shift. Such a system is used to ensure that only authorized persons enter or leave the facility or area concerned and to indicate any limitations placed upon access to classified information. DFS procures and issues the badges. Personal recognition may be used in lieu of a pass or badge system to control access to a facility in which fewer than 30 persons are employed per shift.

NRC Permanent Identification Badge (1)

Issuance (a)

To control access to NRC facilities, the NRC permanent identification badge is issued to all NRC employees, selected NRC contractors, and others, such as long-term visitors and other agency employees assigned to NRC.

Specifications (b)

The face of the badge will contain the name and location of the issuing office, such as NRC headquarters or the regional office, will be consecutively numbered to ensure accountability, and will be prominently coded by letter, number, or color to denote the level of access authorization, if any, held by the person. A clear image of the individual and their name will be as large as practicable. The badge will be designed and made of materials to effectively prevent attempted alteration. Any additional specifications will be developed and approved by DFS.

NRC Visitor Badges *(2)*

Temporary Visitor Badges (a)

Temporary badges are issued to visitors who require one-time or short-term access to NRC facilities. These badges must be continuously and conspicuously worn by the visitor. Temporary badges must be inventoried and accounted for on a daily basis. The inventory of temporary badges will be stored in a locked cabinet when unattended to ensure against loss, theft, or unauthorized use. The NRC temporary visitor badge will contain the following information:

Personnel Identification System (B) (continued)

NRC Visitor Badges (2) (continued)

- Level of access authorization, if any, prominently coded by letter, color, or number (i)
- Escort requirement, if any (ii)
- A control number and/or date to ensure proper facility access and badge accountability/inventory control (iii)

Long-Term Visitor Badges (b)

Long-term visitor badges will be issued only to those persons who have a continuous and recurring need to enter NRC facilities for official business. These badges will conform to the specifications and requirements of Section (B)(1) of this part. Long-term visitor badges will be surrendered at the issuing guard or receptionist desk at the end of the visit or when the visitor no longer requires access to NRC facilities. (i)

Foreign nationals who are temporarily assigned to NRC will be issued a permanent identification badge which meets the specifications and requirements of Section (B)(1) of this part and contains the words "Foreign Assignee." (ii)

Temporary Badges for Employees (3)

Temporary badges for employees must conform to the requirements for permanent hard badges for employees or visitors. Temporary badges for employees must be returned to the guard or receptionist desk at the facility from which they were issued.

Records (4)

Records must be maintained by each facility showing the disposition of all badges and passes in use or in storage. These records must include the date of issuance, the name of the holder, the type of access authorization and, if applicable, the categories of information and the areas within the facility to which access is permitted. Accountability for badges destroyed, scrapped, or returned must be maintained.

Personnel Identification System (B) (continued)

Lost Badges or Passes (5)

Each individual issued an NRC badge or pass is responsible for its protection. The loss or recovery of an NRC identification badge or pass must be reported immediately to DFS.

Recovery (6)

All badges or passes issued must be returned to DFS upon the termination of an individual's employment or when the badge or pass is no longer needed for access to NRC facilities.

Reissuance of Badges or Passes (7)

To maintain effective security, all employee, contractor, and temporary badges or passes in use will be replaced by a badge or pass that is distinctly different in design approximately every 5 years.

Special Requirements for Security Areas (8)

The NRC badge or pass must be shown to the guard, receptionist, or other responsible individual before gaining access to any NRC security area. Badges or passes must be conspicuously worn by all individuals while in any NRC security area. In some instances, or as required by DFS, separate entry registers or logs for the security area also will be used. All employees and duly authorized visitors will be informed of the special security requirements of each security area before being admitted to the area. This instruction is normally accomplished by the guard, the receptionist, or other responsible individual controlling access to the security area concerned.

Physical Barriers (C)

Physical barriers such as walls, doors, fences, and electronic entry devices will be used to deny or impede unauthorized access to security areas or other areas as required by DFS. Permanent barriers will be used to enclose all security areas, and any other area as directed by DFS, except during construction when temporary barriers may be erected. (1)

DFS will approve use of electronic and electro-mechanical devices to control personnel access, such as card reader entry controls, to supplement existing physical security requirements. These devices will be used at those facilities at which physical layout, level of classified

Physical Barriers (C) (continued)

information in use or in storage, and other factors demonstrate that these devices will effectively and efficiently control personnel access to the facilities. The following requirements will apply: (2)

- **General Requirements** (a)

  Entry control devices may be used, as approved above, to control access to NRC-owned or -leased space but must not be used as the sole personnel access control to security areas or other areas in which access to a room or a defined space would constitute access to classified information. (i)

  NRC employees and others who have been authorized unescorted access and whose duties require daily or regular access to facilities or areas employing these devices will be issued the necessary control card or other medium needed to operate the devices. (ii)

- **Requirements for Visitors** (b)

  Visitors requiring access to areas or facilities employing electronic and electro-mechanical devices must report to the appropriate guard or receptionist desk to complete the required visitor sign-in process. Visitors who are authorized unescorted access will be issued a temporary control card/badge. Upon completion of the visit, the temporary control card/badge must be returned to the issuing guard or receptionist desk. (i)

  At certain NRC locations in which the volume of classified information is limited, or in which other supportive physical security measures are used, electronic and electro-mechanical devices may serve as the primary system for controlling personnel access. At these locations, visitors will be admitted by the NRC employee to be visited, but they must be escorted or kept under constant employee observation while in an NRC controlled area. Except as authorized by DFS, employees must not admit visitors to these locations during other than normal business hours. Facility-specific visitor register procedures also must be followed, as appropriate. (ii)

- **Prohibitions** (c)

  Permanent or temporary control cards/badges are not transferable and must not be used by any person who was not originally assigned the use **of** the card/badge. Failure to abide by this requirement will constitute a breach of established security regulations and may result in disciplinary action.

Intrusion Detection (D)

Interior Protective Alarms (1)

As used in this section, devices and equipment for interior intrusion detection systems required for the protection of classified information are tamper-indicating, electrical, electro-mechanical, electro-optical, electronic, or similar devices that will detect intrusion by an individual into the protected facility or area and will alert guards, watchmen, or other duly assigned personnel by means of actuated visible and audible signals.

Access Authorization Requirement (a)

Facility protective personnel responding to intrusion detection alarms used for the protection of National Security Information or Restricted Data must possess "Q" or "L" access authorizations, except in those situations in which a commercial response force, located at a central alarm station outside the facility, is involved. In these instances, the responding **commercial** force must secure the perimeter of the area or facility until properly authorized facility protection personnel arrive. Section (E) of this part sets forth additional specifications for access authorization.

Records (b)

Protective personnel must record each nonscheduled alarm, showing the date and time the signal was received, the time protective or other responsible personnel arrived at the alarmed area, the action taken, and the cause of the alarm if known, or probable cause if the cause is not definitely established. The name and signature of the recorder and the date of the recording must appear in the record.

Reports (c)

A report of each nonscheduled alarm containing the information required in Section (D)(1)(b) of this part must be furnished to the facility security officer immediately if unauthorized intrusion is involved. Otherwise, the report will be furnished to the facility security office on the same day if the alarm occurs during normal working hours or no later than the first working day after the alarm if it occurs during nonworking hours. A violation must be reported immediately (see Part V of this handbook).

Intrusion Detection (D) (continued)

Interior Protective Alarms (1) (continued)

Protection of Central Station Alarm System (d)

Facility central stations must be established as, or located within, security areas and must be constantly attended. Admittance must be restricted to those who require access in the performance of official duties. The number of personnel who require access must be kept to a minimum. (i)

Commercial central stations must meet Grade "A' standards established by Underwriters Laboratory UL-611, "Central Station Burglar Alarm Units and Systems." A copy of UL certification that a central station of a commercial protection service meets these standards will be accepted as evidence of compliance with the requirement. (ii)

Police central stations are normally attended continuously. If response by police to an alarm device is required for NRC facility approval, the central station should be one that is constantly attended by members of the police department who can direct a response by armed policemen to the alarmed area. In addition, the connection to the police central station should meet the specification contained in UL Class A of UL-365, "Police Station Connected Burglar Alarm Systems and Units." (iii)

Protective Lighting (2)

Protective lighting should be used, as appropriate, as part of a security system to properly protect a facility that houses classified information. (a)

Adequate illumination must be provided, as applicable, to detect intruders, reveal unauthorized personnel and permit examination of credentials, personnel identification badges, and vehicles at pedestrian and vehicular entrances. (b)

Protective Personnel

Guard Force

A licensed and trained guard force is required for the protection of security areas in which classified information cannot be adequately safeguarded by employees during working hours or by alarm protection

Protective Personnel (E) (continued)

Guard Force (continued)

systems during nonworking hours as set forth in Section (D) of this part. Guard force requirements (e.g., post orders, performance measures, and other qualifications) must be specified in contract documents.

Protection of Classified Information in Use (F)

Requirements (1)

Persons using classified information in the performance of official duties shall physically protect the information to ensure that the information is safeguarded against unauthorized disclosure. The requirements specified below must be followed by all those who use classified information.

Visual Controls (a)

All classified information must be kept under the constant surveillance of an authorized person. ***As*** specified in Section (G) of this part, classified information must never be left unattended when in actual use and not secured in an approved storage area or container.

Personal Responsibility (b)

Those attending or controlling classified information in actual use shall prevent unauthorized persons from having access to the information. The information must be protected against visual access when the information can be obtained by observation. The information must be covered, turned face down, placed in approved storage containers, or otherwise protected when unauthorized persons are present. As applicable, drapes, blinds, shades, or other window coverings must be drawn to ensure that classified information in use is not viewed by unauthorized persons. Classified information must be returned to approved storage containers or areas as soon as practicable after use.

Accountability (c)

An accountability system must be maintained to promptly reveal when classified information is lost or unaccounted for. The approved NRC accountability system for classified information is specified in Management Directive (MD) 12.2, "NRC Classified Information Security Program."

Protection of Classified Information in Use (F) (continued)

Destruction of Classified Information (2)

When no longer needed, classified information must be destroyed, altered in content or configuration, or otherwise changed ***so*** that the information is completely obliterated or destroyed. The method of destruction chosen must preclude recognition or reconstruction of the classified information involved. Shredding may be used if the shredding device has been approved by DFS. Before destruction, persons should refer to Handbook 12.2, Part I, for itemized destruction procedures for Top Secret, Secret, and Confidential information.

Classified Conferences (3)

Basic Considerations (a)

Conferences involving classified information must be held within NRC-approved security areas whenever practicable. Classified conferences held outside security areas must only be held under conditions in which adequate protection can be provided the classified information **and** with DFS authorization.

Request for Authorization (b)

Requests to hold classified conferences outside NRC security areas must be submitted to the Director, DFS, at least 15 days before the date of the conference and must contain the following information, as appropriate: (i)

- Purpose and nature of conference ***(a)***
- Number of participants *(b)*
- Specific location of conference, that is, building and room number **(c)**
- Level and category **of** the classified information involved *(d)*
- Description of existing security restrictions concerning the classified information involved ***(e)***
- Name of person(s) responsible for the security of the conference **(f)**
- Description of the conference area, adjacent rooms or areas, and the security precautions planned ***(g)***

Protection of Classified Information in Use (F) (continued)

Classified Conferences (3) (continued)

- Information concerning any permanently installed public address systems, telephones, or other known situations or fixtures of possible coricern to the security of the conference *(h)*

Special Note: Requests to hold classified conferences outside security areas must be marked and handled as **Official Use Only** information, except in those instances in which the request contains classified information necessitating security classification and control. (ii)

Other Considerations (c)

The conduct of a classified conference will be based on the following principles:

- All attendees must have the appropriate access authorization and need-to-know. The requirements of MD 12.3, "NRC Personnel Security Program," Part **II** of this handbook, as applicable, also must be met. (i)

- Unless specifically authorized by DFS, all attendees at such events must be U.S. citizens. (ii)

- Before classified information is introduced into a conference situation and as needed throughout the conference, the individual responsible for the security of the conference shall advise those present of the restrictions governing the information. Additional instructions governing the security of the information, such as the permissibility of taking written notes, must be provided as necessary. (iii)

Prevention of the Use of Surreptitious Listening Devices (4)

Offices or rooms within NRC security areas in which Top Secret information is discussed on a regular or recurring basis must be inspected periodically by DFS to ensure that classified information will not be compromised by surreptitious listening devices. The person assuming cognizance over the classified conference shall contact DFS in advance to arrange for security inspection of the office or room. (a)

Protection of Classified Information in Use (F) (continued)

Prevention of the Use of Surreptitious Listening Devices (4) (continued)

Conference rooms located **outside** NRC security areas must be inspected by DFS immediately before any conference involving Top Secret information. Conference rooms used for discussions of Secret information must be inspected periodically and immediately before any Secret discussion. (b)

Inspections of telephone equipment and public address systems must be conducted by appropriately cleared and qualified NRC personnel and contractors, or telephone company personnel. (c)

Telephones or public address systems in conference rooms or offices in which classified discussions regularly occur should be equipped with jacks or other disconnecting devices. Telephones and public address systems must be disconnected when classified discussions are taking place. (d)

Photocopy Machine Control (5)

Reproduction of classified information must be accomplished under appropriate security conditions to preclude unauthorized access. For example, reproduction must not take place in the presence of uncleared persons, care must be taken that no classified waste is trapped in the equipment, and the machine must be cleared of any possible residual classified images by running an unclassified sheet through the machine following classified reproduction. (a)

Machines repeatedly used for reproduction of classified information should be located within a security area and protected against unauthorized access during nonworking hours. Notices regarding the restrictions and requirements of reproducing classified information must be conspicuously posted next to the equipment. Copies of these notices can be obtained from DFS. (b)

Storage of Classified Information (G)

The classification level of classified information determines the protection required for storage.

Storage of Classified Information (G) (continued)

Security Containers (1)

Security containers for Top Secret and Secret information must, as a minimum, be one of the following types:

- **Security Filing Cabinet** (a)

  A security filing cabinet bears a Test Certification Label on the side of the locking drawer, inside the wall adjacent to the locking drawer, or on an interior door plate, or is marked "General Services Administration Approved Security Container" on the exterior of the top drawer or door.

- **Safe (b)**

  A safe is a burglar-resistive cabinet or chest that meets Federal Specification AAF-358 and that bears a label of the Underwriters Laboratories, Inc., certifying the unit to be a TL-15, a TL-30, or a TRTL-30, or bears a Test Certification Label on the inside of the door or is marked "General Services Administration Approved Security Container," exclusive of bolt work and locking devices.

- **Vault** (c)

  Avault is 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 when delay time is assessed in conjunction with detection and communication subsystems of the physical protection system.

- **Vault-Type Room** (d)

  Avault-type room has a combination lock door and is protected by an intrusion alarm system that alarms upon the unauthorized penetration by a person anywhere into the room.

- **Other Repositories** (e)

  Other repositories are those that would provide comparable physical protection in the judgment of **DFS.**

Storage of Classified Information (G) (continued)

Requirements for Storage (2)

The following storage requirements will apply to the storage of classified information:

- **Top Secret Information** (a)

  While unattended or not in actual use, Top Secret information must be under continuous guard control or stored in approved security containers that are—

  - Located within a security area under either central station alarm protection specified in Section (D) of this part or subject to guard patrol and inspection at intervals not to exceed *2* hours (i)
  - Not located within a security area but under central station alarm protection as specified in Section (D) of this part **and** subject to guard patrols at intervals not to exceed *2* hours (ii)

- **Secret Information** (b)

  While unattended or not in actual use, Secret information must be stored in a manner authorized for Top Secret information, or at least as securely as in one of the following methods:

  - If **not** located in a security area, Secret information will be stored in an approved security container under alarm protection as specified in Section (D) of this part, **or** stored in a security container and subject to guard or watchman patrols at intervals not to exceed **4** hours. (i)
  - If located within a security area, Secret information will be stored-(ii)
    - **As** specified in Section (G)(2)(b)(i) of this part or in a commercial-type steel filing cabinet equipped with a built-in combination lock and under either alarm protection as specified in Section (D) of this part or subject to guard or watchman patrols at intervals not to exceed 8 hours *(a)*
    - In unlocked cabinets or open storage, such as shelves and bookcases, within a vault-type room *(b)*

Storage of Classified Information (G) (continued)

Requirements for Storage (2) (continued)

- In a combination-padlocked filing cabinet under alarm protection as specified in Section (D) of this part and subject to guard or watchman patrols at intervals not to exceed 8 hours (c)

- **Confidential Information** (c)

  While unattended or not in use, Confidential information must be stored in a manner authorized for Top Secret or Secret information, or at least as securely as in one of the following methods:

  - In a commercial-type steel filing cabinet equipped with a built-in combination lock (i)
  - In unlocked cabinets or open storage within a locked room or in a key-locked filing cabinet **and** the room or cabinet is under alarm protection as specified in Section (D) of this part (ii)

- **Communications Security (COMSEC) Information** (d)

  While unattended or not in use, COMSEC information must be stored in a manner authorized above for the classification involved and storage must meet the standards and specifications set forth in NACSI-4005 (published by the National Security Agency, Department of Defense) and MD 12.4, "NRC Telecommunications Systems Security Program."

- **Sensitive Compartmented Information** (e)

  Sensitive compartmented information facilities must be afforded physical protection as required by Directive 1/21, "Physical Security Standards for Sensitive Compartmented Information Facilities (SCIF)," Director of Central Intelligence, July 29, 1994. Matters pertaining to security requirements for these facilities must be directed to the Director, DFS, for coordination.

- **Repository Checks** (f)

  When guards or watchmen are required for the protection of NRC classified information in facilities housing unalarmed repositories containing Secret or Confidential information, the guards or watchmen shall—

Storage of Classified Information (G) (continued)

Requirements for Storage (2) (continued)

- Physically inspect these repositories as soon as possible after the close of each working day and at least once every 8 hours during a Saturday, Sunday, holiday, or other nonworking day (i)
- In the' case of repositories located within security areas, physically inspect the entry into the security area or the repository itself, whichever applies, at intervals not to exceed **6** hours (ii)

Alternate Storage Locations (3)

Safe deposit boxes or vaults of a bank may be used for storage of Secret or Confidential information provided that the lock and keys to the box or vault are changed before use and the customer's key is furnished only to those authorized access to the contents. These persons shall be appropriately cleared for the level of classification involved. (a)

Remote storage facilities, such as an offsite emergency relocation center or an underground Federal facility in a remote location, must be equipped with security containers for the storage of classified information and must otherwise meet the requirements of Section (G)(2) of this part. **(b)**

DFS can arrange for the storage of NRC Secret and Confidential documents in certain Federal records centers (FRCs). Among other necessary conditions for this storage are General Services Administration approval for storage of the category and level of classified information involved, and DFS approval of the FRC facility in accordance with Part I of this handbook. If a problem involving volume storage of classified documents can be alleviated by FRC storage, contact DFS for additional guidance. (c)

Miscellaneous Storage Specifications and Procedures (4)

Combination Locks (a)

A combination lock is a three- or four-position, dial-type combination lock meeting Federal Specification FF-L-2740. (i)

A combination padlock is a three-position, dial-type, changeable combination padlock meeting Federal Specification FF-P-110. (ii)

Storage of Classified Information (G) (continued)

Miscellaneous Storage Specifications and Procedures (4) (continued)

Combinations of locks or padlocks on repositories containing classified information may be known only by those authorized access to the information and must be changed when repositories are placed in use, whenever anyone knowing the combination terminates employment, whenever the combination may have been compromised, or at least every **3** years. See Section (G)(4)(c) of this part for additional information regarding combinations. (iii)

Records of combinations must be classified no lower than the highest classification of the information stored in the repository. (iv)

Lock Bars, Keys, Hasps, and Yokes (b)

Lock bars must be **1-1/4** inches by **3/16** inch or equivalent in cross-section and constructed of hardened steel or a material of equivalent hardness. (i)

Hasps and yokes on repositories containing classified information must be constructed of hardened steel at least **1/4** inch in diameter or equivalent cross-section and secured to the repositories by welding or riveting. (ii)

Keys to locks used to secure gates or doors in the perimeters of a security area must be issued only to those authorized access to the information or to the area. Keys must be given protection equal to that afforded the information or item being protected. A record of all locks, cores, and keys must be maintained. Keys must be recovered from terminating personnel. Locks must be changed or recorded immediately whenever a key is lost, the key or lock has been compromised, or when unrecorded keys are found. A physical inventory of locks, cores, and keys must be conducted annually. (iii)

Locking and Monitoring of Repositories and Office Areas (c)

Each office must assign personnel to lock and monitor the locking of all repositories containing classified information and to ensure that all classified information is properly secured when the office is unattended. (i)

The names, addresses, and home telephone numbers of custodians having knowledge of the combination and the date of the last combination change must be posted on the inside of each classified

Storage of Classified Information (G) (continued)

Miscellaneous Storage Specifications and Procedures (4) (continued)

repository on Part I of SF 700, "Security Container Information" (Exhibit 3). Part 2A contains the combination of the repository and must be classified at the highest level of the information authorized for storage in the repository. Part 2 must be similarly classified at the highest level of the information authorized for storage in the repository when it contains the combination. A new SF 700 must be completed each time the combination of the repository is changed. (ii)

SF 702, "Security Container Check Sheet" (Exhibit 4), must be posted on each repository containing classified information. The check sheet must be initialed at the end of each workday in the "closed by" block by the person responsible for locking the repository and in the "checked by" block by one other person who has physically checked the repository to ensure that it has been properly secured. If no other person is available, the person locking the repository will recheck the repository and initial the "checked by" block as well as the "closed by" block. (iii)

Security containers that must be removed for repair or maintenance, or are to be returned to the supply system, or are taken out of service for any reason must be physically examined by the custodian of the container before this action to ensure that no classified information is mistakenly left in the container. Any built-in combination lock must be reset to the standard combination *50-25-50*. Combination padlocks must be reset to the standard combination 10-20-30. (iv)

Unattended Repository Found Open (d)

In the event an unattended repository containing classified information is found open, a card, "Notice of Unlocked Condition-Classified Matter Container," is placed in the repository, the repository is secured by a designated person such as a guard or watchman, and the custodian shall check the contents not later than the next workday. (i)

If there is an indication of a suspected violation (see Part V of this handbook) by NRC employees or contractors, it must be reported immediately to DFS and the Office of the Inspector General (OIG). Personnel must secure the area, being careful not to destroy any criminal evidence, but independent investigations shall not be conducted before notifying DFS and OIG. (ii)

Trespassing on Commission Property (H)

Statutory Provisions (1)

Pursuant to the authority of Section **229** of the Atomic Energy Act of **1954,** as amended, 10 CFR Part 160 prohibits the unauthorized entry and the unauthorized carrying, transporting, or otherwise introducing or causing to be introduced any dangerous weapon, explosive, or other dangerous instrument or material likely to produce substantial injury or damage to persons or property, into or upon any designated and posted facility, installation, or real property subject to the jurisdiction, administration, or in the custody of the Commission. The statute provides penalties for violations.

Criteria (2)

Selection of facilities, installations, and real property for posting will generally be based upon the need for supplementing other Federal statutes protecting against espionage, sabotage, or destruction of Government property. Real property may be posted for protection for reasons other than the protection of classified information if deemed necessary.

Proposals (3)

Submission (a)

Proposals for the posting of facilities, installations, or real property, or amendment to or revocation of a previous proposal, will be submitted when-

- The property is owned by, or leased to, the United States for use by the NRC. (i)
- The property requires protection under 10 CFR Part 160. (ii)
- **A** previous notice needs to be amended or revoked. (iii)

Contents (b)

Each proposal for posting will contain the name and specific location of the installation, facility, or real property to be covered, and the boundary coordinates. If boundary coordinates are not available, the proposal will include a description adequate enough to furnish reasonable notice of the area to be covered, which may be an entire area or any portion thereof that can be physically delineated by the posting specified in Section **(H)(4)** of this part. (i)

Trespassing on Commission Property (H)(continued)

Proposals (3) (continued)

Each proposal for amendment or revocation will identify the property involved; state clearly the action to be taken, such as a change in property description, correction, or revocation; and contain a new or revised property description, if required. (ii)

Posting Requirements (4)

Upon approval by the Executive Director for Operations (EDO), the notice designating the facility, installation, or real property, or amending or revoking a previous notice, will be published in the *Federal Register*. The regulation will be effective 30 days after publication, provided the posting requirements are accomplished. (a)

If directed by the EDO, property covered under 10 CFR Part 160 will be posted at entrances and at intervals along the perimeter of the property to provide reasonable assurance of notice to persons about to enter the property. Signs will measure at least 11 by 14 inches reading as follows: (b)

NO TRESPASSING
BY ORDER OF
THE UNITED STATES
NUCLEAR REGULATORY COMMISSION

The unauthorized entry upon any facility, installation, or real property subject to the jurisdiction, administration, or in the custody of the Nuclear Regulatory Commission that has been designated as subject to the provisions contained in Part 160 of the rules and regulations of the Nuclear Regulatory Commission (10 CFR Part 160) is prohibited, and the unauthorized canying, transporting, or otherwise introducing or causing to be introduced any dangerous weapon, explosive, or other dangerous instrument or material likely to produce substantial injury or damage to persons or property, into or upon such facility, installation, or real property is prohibited.

Whoever willfully violates the aforesaid regulation of the Nuclear Regulatory Commission shall, upon conviction thereof, be punishable by a fine as specified in 10 CFR 160. whoever willfully violates this regulation with respect to any facility, installation, or

Trespassing on Commission Property (H) (continued)

Posting Requirements (4) (continued)

real property enclosed by a fence, wall, floor; roof or other structural barrier shall be guilty of a misdemeanor and, upon conviction thereof, shall be punished by a fine of not to exceed $5,000 ***or*** *imprisonment for not more than 1 year;* ***or*** *both.*

By authority of Section 229 of the Atomic Energy Act of 1954, as amended, and Part 160 of the rules and regulations of the Nuclear Regulatoiy Commission, this facility, installation, ***or*** *real property has been designated as subject to these regulations by the Nuclear Regulatoiy Commission.*

Notification of the Federal Bureau of Investigation *(5)*

Notification of the date of posting, relocation, removal of posting, or other change in the identity of the property involved must be furnished promptly to the local office of the Federal Bureau of Investigation exercising investigative responsibility for the property.

Violations (6)

Violations of the prohibitions as posted must be reported in accordance with Part V of this handbook.

Part III
Protection of Unclassified NRC Facilities

This part provides guidance for those responsible for the protection of NRC facilities that are not protected as security facilities under Part I of this handbook but that require safeguarding to ensure adequate protection of NRC property and programs.

Criteria (A)

Facilities that are not protected as security facilities under Part I of this handbook require protection commensurate with their monetary value or programmatic importance. For the purposes of this part, an unclassified NRC facility requiring protection is any facility that—(1)

- Contains property, excluding real property, owned by or leased to the NRC, valued at $1,000,000 or more (a)
- Contributes in an important manner to fulfilling NRC's responsibility for the protection of public health or safety (b)
- Assumes importance for continuity of NRC programs or is essential to the NRC mission (c)
- Is determined by the Director, Division of Facilities and Security (DFS), Office of Administration (ADM), for headquarters facilities or by the responsible regional administrator for facilities within the region's geographical area of responsibility to require protection for other reasons (d)

When the relative importance of an unclassified NRC facility does not fall under these criteria, the facility must be protected to a degree called for by its value and significance. The extent of and need for protective measures at such a facility must be determined by the appropriate responsible NRC official, either the Director, DFS, for a headquarters facility or the regional administrator for a regional facility. (2)

Guidance (B)

General (1)

Protective measures must be taken to prevent loss, damage, or destruction that might result from theft, vandalism, arson, sabotage, or other unlawful acts at unclassified NRC facilities. The measures taken must be adequate to provide reasonable assurance of protection and may include access controls; physical barriers, such as walls and fences; guards or watchmen; lock and key systems; and intrusion alarms.

Standards and Requirements (2)

Access Controls (a)

Access to an unclassified NRC facility must be controlled during working hours by receptionists or by employees who have been specifically designated responsibility for ensuring that only those with proper authorization are admitted. When the facility is unoccupied, such as during nonworking hours, or occupied by a small number of persons unable to afford adequate protection, these facilities, as a minimum, must be locked with NRC-approved locking devices and must be protected by other means, such as NRC-approved access control devices, designated by the Director, DFS, or the responsible regional administrator, as appropriate.

Physical Barriers (b)

Barriers such as walls and fences are intended to control or impede access. Walls of buildings normally constitute an adequate physical barrier. When the size or nature of the facility warrants, fencing may be required and must be approved by the Director, DFS, or the regional administrator.

Guards or Watchmen (c)

Protection may be provided by guards or watchmen as the Director, DFS, or the responsible regional administrator deems necessary. When guards or watchmen are used, patrols must be conducted at irregular intervals but not less frequently than once every 8 hours during nonworking or unoccupied periods.

Guidance (B) (continued)

Standards and Requirements (2) (continued)

Locks and Keys (d)

Key locks in doors must be resistant to picking and jimmying. Combination locks must be resistant to manipulation. Padlocks must be of sturdy construction and resistant to picking, rapping, forcing, or the use of shims or similar techniques. Hasps and other door hardware must afford equivalent protection, as appropriate. Positive control of keys is essential. When an exterior or outer perimeter entrance key or door key is lost and there is reason to believe it has been compromised, the lock that it opens must be replaced or recorded immediately. Combinations or keys and cores of exterior entrances or doors must be changed when a person having access thereto is terminated or the person is permanently reassigned to another facility. Locks must be replaced or recorded, or combinations changed for interior doors whenever 5 percent of the keys are lost or whenever the management official responsible for the area deems it appropriate. Advice on approved locks is available from DFS.

Intrusion Alarms (e)

Alarm systems may be used to provide or supplement notification of an actual unauthorized entry into an NRC facility or onto its premises. ***An*** intrusion alarm system is considered to be of significant value when a response time not exceeding 15 minutes is ensured and when the system itself is dependable. DFS can advise on alarm systems.

Prohibited Articles *(f)*

Inspection of packages to ensure that prohibited articles are not introduced into the facility must be accomplished as specified in Part II of this handbook.

Signs Posting "No Trespassing" (g)

Facilities owned or leased by NRC must be posted as specified in Part **II(H)(4)** of this handbook.

Guidance (B) (continued)

Standards and Requirements (2) (continued)

Reports (h)

Incidents bearing on the security of the facility, such as fire, vandalism, bomb threats, riots or civil disturbances, must be reported immediately to DFS by telephone and also to the responsible regional office, if appropriate. This report must be promptly followed up in writing and must be initiated by the responsible NRC organization monitoring NRC's interest at the facility.

Surveys (i)

Physical protection surveys of unclassified NRC facilities must be conducted as specified in Part I of this handbook.

Occupant Emergency Program (C)

In accordance with Federal Property Management Regulations promulgated by the General Services Administration (GSA) **(41** CFR **101-20.5),** an occupant emergency program must be established at all NRC **federally occupied** facilities, regardless of their designation as either security facilities under Part I of this handbook or as unclassified NRC facilities as stated in this part.

Occupant Emergency Plan (1)

An occupant emergency plan (OEP) specifies responses in an emergency situation and methods to protect life and property in a specific federally occupied space. For NRC headquarters related buildings, OEPs are developed and coordinated by DFS and approved by the Director, ADM, and local fire/rescue authorities. NRC regional offices develop, coordinate, and seek approval of their OEPs through their local GSA regional office.

Occupant Emergency Program (C) (continued)

Designated Official (2)

As defined in **41** CFR **101-120.5,** the designated official is the highest ranking official of the primary occupant agency or the alternate highest ranking official or designee selected by mutual agreement by other occupant agency officials. The designated official is responsible for developing, implementing, and maintaining a current OEP and for establishing, staffing, and maintaining the occupant emergency organization.

Non-Federal Facility Emergency Plan (D)

To ensure that emergency situations are appropriately provided for, non-Federal facilities, such as those of an NRC contractor, falling within the purview of this part must establish an adequate emergency plan to provide for the prompt assistance of Federal, State, and local law enforcement authorities and other emergency assistance organizations. **DFS** will review and approve this emergency plan during physical protection surveys and DFS will advise as to the specific content of the plan on a case-by-case basis. Generally, these plans cover-

- The emergency chain of command **(1)**
- Designation of specific individuals, with alternates, who are responsible for key emergency functions and for notifying DFS or the appropriate regional administrator of incidents bearing on the security of the NRC interest at the facility **(2)**

Part IV

Security Awareness

This part specifies the policy and requirements for a security awareness program to: develop an appreciation for the importance of security and the importance of potential threats to security; provide employees with an understanding of security policies, procedures, and requirements; advise employees of their security responsibilities; and ensure adequate protection for classified and sensitive unclassified information and NRC property.

Program Design (A)

The program must be developed and implemented with careful consideration of—(1)

- The categories and quantities of classified or sensitive unclassified information handled and the personnel involved (a)
- The physical security aspects of the facility (b)
- Existing personnel security access authorization requirements (c)

The program must employ methods that are appropriate and effective for the personnel and situations concerned. The methods may range from informal instruction of individuals to audiovisual presentations for large groups. Briefing presentations by individuals skilled in public speaking and the use of constructive instruction techniques such as visual aids and audience participation are essential as they increase employee interest, motivation, and knowledge retention. (2)

The program must contain-(3)

- *An* initial security orientation briefing for new and newly assigned employees (a)
- A briefing on safeguarding classified information for newly cleared employees (b)

Program Design (A) (continued)

- Continuing and special security awareness efforts (c)
- A final briefing upon termination of an individual's NRC access authorization (d)

The Director, Division of Facilities and Security (DFS), will approve or disapprove the use of classified information for security awareness needs consistent with the requirements **of** this part. (4)

Program Components (B)

Security Orientation Briefing for New Employees (1)

A security orientation briefing must be given by an employee or a representative of DFS to NRC employees when they start duty and by the contractor security officer to contractor employees who have been granted an NRC access authorization. This briefing will contain the following:

- The types of security clearances granted by the NRC and the access those clearances afford after an official need-to-know has been established (a)
- Personnel security reporting responsibilities of each individual (b)
- Prescribed procedures for the storage and handling of sensitive unclassified information and the importance of protecting this information (c)
- Physical security aspects of the particular facility, the importance of visitor control, and the means or procedures for protecting Government property (d)
- Information on where to obtain further guidance or assistance (e)

Briefing on Safeguarding Classified Information (2)

A briefing on safeguarding classified information will be given by an employee or a representative of DFS to NRC employees who have been granted an NRC access authorization. This briefing will contain the following:

Program Components (B) (continued)

Briefing on Safeguarding Classified Information (2) (continued)

- Requirements for access to classified information (a)
- Types and levels of classified information (b)
- Prescribed procedures for the storage, handling, and transmission of classified information and the importance of protecting this information (c)
- Information on where to obtain further guidance or assistance, such as MD 12.1 or consulting an authorized classifier or a security advisor (d)
- The requirement for signing an SF 312, "Classified Information Nondisclosure Agreement" (Exhibit ***5)*** (e)

Continuing Refresher or Special Security Awareness Efforts (3)

Security Advisor Program (a)

The objectives of the security advisor program are to increase the understanding of and compliance with NRC security policies and procedures; to provide readily available security advice and assistance throughout the NRC organization; and to expand communications between DFS and NRC employees. One or more employees from each NRC organizational component and the regional offices are appointed to serve as security advisors for the employees of their organizational component or region. DFS will adequately acquaint these individuals with basic and general NRC security policies and procedures and the staff and functions of DFS. Further, DFS will keep the security advisors informed of revision to security procedures and requirements and items and occurrences of security interest or concern.

On-the-Job Security Training (b)

Supervisors shall supplement the security education and awareness program through demonstrated endorsement of security principles and procedures, and by providing specific on-the-job instructions pertinent to the sensitivity of the employee's position and duties, such as protection requirements for information handled. *Also,* any physical security procedures particular to the office will be explained.

Program Components (B) (continued)

Continuing or Special Security Awareness Efforts (3) (continued)

Special Briefings (c)

DFS shall develop and present special briefings as requested by management, when a specific need is recognized, or in support of other security programs such as the authorized classifiers program. Contractor security officers should contact DFS when special briefings are requested or considered.

Defensive Security Briefings (d)

Through various security education efforts, NRC and contractor employees who have been granted an NRC access authorization will be encouraged to contact DFS or their security officer, respectively, when they contemplate travel, either official or personal, to designated countries or attendance at any international meeting, conference, or symposium so that they can be given a defensive security briefing.

Publications and Other Media (e)

Publications and other media, such as posters, audiovisual productions, and booklets may be used in support of the Security Awareness Program to increase employee awareness, employee motivation, and program effectiveness.

Briefing on Termination of Access (4)

When an individual's NRC access authorization is to be terminated in accordance with MD 12.3, "NRC Personnel Security Program," DFS, or designated regional staff, will conduct a termination briefing to inform the individual of his or her continuing security responsibilities. After all statements contained in NRC Form 136, "Security Termination Statement" (accessed through the Wordperfect Informs icon), have been reviewed, the terminating individual and the person conducting the briefing shall execute the form.

Program Records (C)

NRC employees and contractors to whom an access authorization has been granted shall complete an SF 312, "Classified Information Nondisclosure Agreement" (Exhibit 5), upon attendance at the briefing on safeguarding classified information; and an NRC Form 136 upon termination of NRC employment. The original copy of these

Program Records (C) (continued)

completed forms will be forwarded to DFS for retention. The NRC Form 136 is retained in the individual's personnel security file and the SF 312 is retained in a separate file system maintained by DFS. (1)

NRC contractors shall maintain records of an employee's orientation, refresher, or special security briefings related to NRC work performed, and of the termination briefing, for 1 year after termination of the employee's NRC access authorization. The original copy of the completed NRC Form 136 must be forwarded to DFS for retention in the employee's personnel security file; the original copy of the completed SF 312, if applicable, must be forwarded to DFS for retention. (2)

Part V

Infractions and Violations

This part contains the requirements, standards, and procedures governing the NRC security infraction program, alleged and suspected violations of laws of security interest, and losses and compromises of classified and sensitive unclassified information.

Infractions (A)

Security Infraction (1)

A security infraction **is** an act or omission involving failure to comply with NRC security requirements or procedures. Therefore, an infraction may include an actual or suspected compromise of classified information or sensitive unclassified information. A security infraction also may constitute a violation under this part.

Administrative Action (2)

Administrative action, which may include disciplinary or adverse action, must be taken in any case in which a person is responsible for an infraction, except for minor infractions not actually jeopardizing the security of classified information or sensitive information. An example of a minor infraction is the failure to place the name of the addressee on a receipt when the receipt is signed by the addressee's authorized representative, or failing to change a repository combination until a few days after the required date.

Infractions (A) (continued)

Administrative Action (2) (continued)

Determination of Action (a)

NRC Employees (i)

Office or division directors at headquarters or regional administrators shall determine whether an infraction committed by an NRC employee requires disciplinary or adverse action and, if so, the severity of the action. The responsible director or administrator shall consult with the personnel office about any contemplated adverse action.

NRC Contractor Employees (ii)

Officials designated by contractors shall determine whether an infraction committed by an NRC contractor employee requires disciplinary or adverse action and, if so, the severity of the action.

Personnel of Other Government Agencies (iii)

The NRC or the NRC contractor shall take the minimum action in the case of personnel of other Government agencies assigned to the NRC or to NRC's contractors for the first infraction as described in Section (A)(2)(c) of this part, unless the first infraction significantly endangers the national security or the security **of** the NRC program. For a first infraction that endangers security and for any subsequent infraction, the responsible NRC official or NRC contractor official shall report the infraction to the Government agency to which the employee is permanently assigned to allow that agency to take the disciplinary or adverse action deemed necessary.

Determining Factors (b)

For NRC personnel or NRC contractor employees, the following factors should be considered in determining the action to be taken on security infractions-

- The degree to which the national security or the security of the NRC program is endangered (i)
- The employee's performance, conduct, attitude, and past record of compliance with security regulations (ii)

Infractions (A) (continued)

Administrative Action (2) (continued)

Suggested Schedule of Administrative Action (c)

Except in cases in which consideration is being given to suspending or terminating access authorization, the following schedule of administrative action is suggested for infractions occurring within any 12-month period.

- **First Infraction** (i)

  Interview the person committing the infraction to impress on that person the seriousness of the matter, determine the reason for the infraction, and call attention to pertinent regulations and office procedures. If necessary, modify office procedures to prevent a recurrence. The following responsible officials will conduct the interviews:

  - **Regions** *(a)*

    - In the case of an NRC regional office employee other than the administrator, the interview will be conducted by the administrator, or the administrator's designee. *(I)*

    - In the case of an infraction committed by the administrator, the interview will be conducted by the person to whom the administrator is administratively responsible. (2)

  - **Headquarters** *(b)*

    - In the case of a headquarters employee other than an office or division director, the interview will be conducted by the director, the deputy director, or the assistant director of the employee's office or division, unless these persons are involved in the infraction. *(I)*

    - In the case of the deputy director or the assistant director, the interview will be conducted by the director. (2)

    - In the case of an office or division director, the interview will be conducted by a person to whom the director is administratively responsible. *(3)*

Infractions (A) (continued)

Administrative Action (2) (continued)

- **Contractors and Other Organizations** *(c)*

  In the case of a contractor employee or an employee of an organization other than NRC, the interview will be conducted by an official designated by the contractor or the organization involved.

- **Second Infraction** (ii)

  Interview the person committing the infraction as specified in Section (A)(2)(c)(i) of this part and write a reprimand to the employee warning that another infraction may result in an adverse action, specifically that the employee may be suspended without pay. Place a notation of the interview and a copy of the written reprimand in the employee's personnel and security files.

- **Third Infraction** (iii)

  Interview the person committing the infraction as specified in Section (A)(2)(c)(i) of this part, suspend the employee without pay for **3** working days, and provide the employee written notification that a subsequent infraction may result in removal from his or her position with the NRC and from Federal service. Place a notation of the interview, a copy of the written reprimand, and a copy of the suspension letter in the employee's personnel and security files.

- **Subsequent Infractions** (iv)

  Determine whether to propose the employee's removal for cause. If the employee's removal is not proposed, propose other appropriate adverse action, such as an additional suspension without pay. Document the action taken in the employee's personnel and security files.

Reporting Infractions (3)

NRC Employees (a)

Office or division directors and regional administrators shall report, in writing, to the Division of Facilities and Security (DFS), Office of Administration, each infraction involving NRC personnel, consultants, and others under their jurisdiction immediately following the infraction.

Infractions (A) (continued)

Reporting Infractions (3) (continued)

Contractor Employees (b)

A contractor shall report each infraction immediately following its occurrence, in writing, to **DFS,** with a copy to the NRC project officer. In addition, the contractor shall immediately notify the contracting officer that an infraction has occurred, the details of the infraction, and the name of person who committed it.

Content of Reports (c)

NRC or NRC contractors shall attach two copies of any associated written reprimand or notice to each report that has been issued and shall forward the report and attachments to DFS to be placed in the individual's personnel security files. The report must state-

- The full name of the individual involved (i)
- The title of that individual's position and the name and title of his or her employer (ii)
- The type and level of information involved, if applicable (iii)
- The date, reason or cause, and nature of the infraction (iv)
- Whether it is the first, second, third, or subsequent infraction within a 12-month period, if known (v)
- The corrective action taken (vi)

Preliminary Inquiry (4)

Upon receipt of the report of an infraction, **DFS,** or personnel designated by **DFS,** such as regional personnel, may conduct a preliminary inquiry to determine the facts and circumstances surrounding the infraction, the person responsible, and the adequacy of security procedures within the organization in which the infraction occurred. **If** at any time during the course of the preliminary inquiry information is developed that suggests a violation may have occurred, the matter will be referred immediately to the Office of the Inspector General (OIG) or the Office of Investigations (0I), as appropriate, for action. See Section (B)(3) of this part.

Violations (B)

Violation (1)

"Violation," as used in this part, covers criminal breach of the Atomic Energy Act of 1954; Internal Security Act of 1950, when related to NRC activities; Title 18 U.S. Code relating to—(a)

- Espionage or information control, Sections 792-98 (i)
- Sabotage, Sections 2151-57 (ii)
- Treason, sedition, and subversive activities, Sections 2381-85 (iii)
- Malicious mischief, Sections 1361-64 (iv)
- Actual or threatened use of explosives against persons or property, Sections 841-48 (v)
- Destruction of Government property, Sections 1361, 2232 (vi)
- Embezzlement and theft, Sections 641-665 (vii)
- Extortion and threats, Sections 871-878 (viii)

Other Federal statutes related to the national security, the security of the NRC program or facilities, or classified information. (b)

Handling a Violation (2)

Alleged or suspected violations of the Atomic Energy Act and other Federal statutes affecting the national security and the security of NRC or NRC contractors must be handled with a view to timely and effective action.

Reporting Procedures (3)

Reports to DFS (a)

Except as stated in Section (B)(3)(c) of this part, NRC or NRC contractor personnel shall immediately report alleged or suspected violations affecting classified information, sensitive unclassified information, and **the** safety **of** NRC personnel or property to DFS for preliminary inquiry and further referral, if warranted.

Violations (B) (continued)

Reporting Procedures (3) (continued)

Reports to OIG and O I (b)

OIG and OI will advise DFS of alleged or suspected violations of security interest reported directly to them.

Reports to the Regional Administrators (c)

For cases requiring prompt field response, NRC employees or NRC contractor personnel under the jurisdiction of a regional administrator shall report alleged or suspected violations such as sabotage, terrorism, or the theft of special nuclear material to the regional administrator. The regional administrator shall notify the local Federal Bureau of Investigation (FBI) immediately and promptly advise OIG or OI, as appropriate, for action.

Method of Reporting (d)

To ensure timely reporting, the initial report will generally be oral; however, reports must immediately be confirmed in writing.

Content of Report (4)

Reports that contain classified or sensitive unclassified information must be properly protected and marked with the appropriate classification and control markings. Reports of alleged or suspected violations not involving losses or compromise of classified or sensitive unclassified information discussed in Section (C) of this part must contain—

- A statement regarding the items and information involved (a)
- Names of personnel involved (b)
- Circumstances (c)
- Action contemplated or taken (d)

Violations (B) (continued)

Investigation of Violations *(5)*

OIG is responsible, except as stated in Section (B)(3)(c) of this part, for investigating and referring to the Department of Justice (DOJ), if necessary, alleged or suspected violations by employees of NRC or NRC contractors. 01 is responsible, except as stated in Section (B)(3)(c) of this part, for investigating and referring to the DOJ, if necessary, alleged or suspected violations that licensees, applicants, and their contractors and vendors commit.

Assistance to Federal Law Enforcement Agencies (6)

The NRC will give Federal law enforcement agencies all appropriate assistance, including technical advisory assistance, as needed. Agents of the Federal Bureau of Investigation (FBI) must be granted admission to all areas and afforded access to any Restricted Data or other classified information or sensitive unclassified information necessary to the performance of their duties. They must be advised at the time of access, either oral or visual access, of the level and category of classification, or of the category of sensitive unclassified information, and the procedures required to protect the information. The availability of NRC badges and advance notification arrangements must be determined by agreements between the NRC and the FBI offices involved.

Followup of Alleged or Suspected Violations of Security (7)

NRC followup will include coordination with FBI or other Federal law enforcement authorities. Followup will be accomplished so as not to interfere with any investigation the FBI or other Federal law enforcement agencies are conducting and will be coordinated between OIG or 01 and DFS as their interests demand.

Losses or Compromise of Classified Information or Sensitive Unclassified Information *(C)*

Reporting Procedures (1)

Any NRC employee or NRC contractor employee who knows of the loss or possible or actual compromise of classified or sensitive unclassified information shall report that fact to DFS by the most rapid and secure means available.

Losses or Compromise of Classified Information or Sensitive Unclassified Information (C) (continued)

Content of Report (2)

The report of a lost or compromised classified or sensitive unclassified document must contain-

- Title, type, and physical form of the document (a)
- **A** brief description of the contents of the document (b)
- Originator's name (c)
- Any identification number and the date of the document (d)
- Level and category of classified information or type of sensitive unclassified information contained in the document (e)
- Names of the person to whom the document was charged and the person responsible for protecting the document ***(f)***
- Last known location of document if a lost document is involved (g)
- Known circumstances surrounding the loss or compromise of the document (h)

Action (3)

Upon notification, DFS will conduct a preliminary inquiry, including a preliminary assessment of the damage to NRC's mission or the national security. DFS will refer the preliminary assessment to the Executive Director for Operations (EDO), OI, OIG, OGC, or the Chairman, as warranted, and take any other appropriate action:

- Whenever the lost or compromised classified information has been originated by or is of interest to another Government agency, DFS will notify each agency involved **of** the facts, circumstances, actions being taken by NRC, and pertinent findings. DFS will also inform the designated representative of the Director, Central Intelligence. (a)

Losses or Compromise of Classified Information or Sensitive Unclassified Information (C) (continued)

Action (3) (continued)

- DFS will determine whether actions taken in response to the loss or compromise of sensitive unclassified information are consistent with the schedule for infractions specified in Section (A)(2) of this part. If statutory penalties such as penalties for disclosure of unclassified Safeguards Information as specified in Section 147 of the Atomic Energy Act and penalties for the unauthorized disclosure of trade secrets as specified in 18 U.S.C. 1905 are involved, DFS will refer the matter to OIG or OI for further referral, notifications, and other necessary actions. (b)

Damage Assessment (4)

When Conducted (a)

If, in the judgment of the Chairman, the EDO, or DFS, after having reviewed the preliminary assessment regarding the compromise of classified information originated by or for NRC, damage to the national security could reasonably be expected, DFS will prepare a damage assessment and take any other action warranted by the damage.

Content of Damage Assessment (b)

Damage assessments must be in writing and, as a minimum, contain the following information:

- Identification of the source, date, and circumstances of the compromise (i)
- Classification of the specific information lost (ii)
- A description of the specific information lost (iii)
- An analysis and statement of the known or probable damage to the national security that has resulted or may result from the compromise (iv)
- An assessment of the possible advantage to foreign powers resulting from the compromise (v)

Losses or Compromise of Classified Information or Sensitive Unclassified Information (C) (continued)

Damage Assessment (4) (continued)

- ***An*** assessment of whether—(vi)
  - The classification of the information involved should be continued without change *(a)*
  - The specific information, or parts thereof, must be modified to minimize or nullify the effects of the reported compromise and the classification retained *(b)*
  - Downgrading, declassification, or upgrading is warranted (If these actions are warranted, promptly notify holders of the information of any change and obtain confirmation of receipt of notification.) (c)
- ***An*** assessment of whether countermeasures are appropriate and feasible to negate or minimize the effect of the compromise (vii)
- ***An*** assessment of other appropriate corrective, administrative, legal, disciplinary, or adverse actions (viii)

Damage Assessment Involving Information From Other Government Agencies (c)

Whenever a damage assessment incorporating information from NRC and one or more other Government agency is needed, DFS and personnel of the other agency shall agree upon the assignment of responsibility for their agency's portion of the damage assessment. If NRC and any other agency conduct separate damage assessments for the same infraction, the NRC and any other agency involved will exchange any information from their separate assessments that would affect another agency's information or interests.

Compromise by Foreign Nationals (d)

Whenever DFS performs a damage assessment involving the compromise of **U.S.** classified information as the result of actions taken by foreign nationals, by foreign government officials, or by **U.S.** nationals in the employ of international organizations, DFS will request that the Office of International Programs (OIP) obtain the

Losses or Compromise of Classified Information or Sensitive Unclassified Information (C) (continued)

Damage Assessment (4) (continued)

required information pertinent to the assessment through appropriate intergovernmental liaison channels. (i)

If NRC and one or more other Government agencies are responsible for the assessment, OIP will arrange for joint preparation of the assessment with any other involved agency through appropriate channels before transmitting the request for joint preparation to the other agency. (ii)

Records Maintained (5)

DFS, OIG, and OI will maintain appropriate records of each instance involving the loss or compromise of classified information. The records must identify the classified information involved, the date on which the loss was discovered or the compromise occurred, any action taken to determine whether the loss or compromise could reasonably be expected to cause damage to the national security, the determinations reached, a copy of the damage assessments in cases of loss or compromise, and any other action taken in each instance.

Actions Against Individuals (6)

Administrative and Criminal Sanctions (a)

Persons determined to have knowingly made an unauthorized disclosure of classified information or who have refused to cooperate in the inquiry or investigation will be denied further access to classified information and may be subject to other administrative sanctions. If alleged or suspected violations of Federal statutes are proven, the administrative or criminal penalties of the statute apply.

Action When No Criminal Prosecution Is Contemplated (b)

Whenever an action, other than criminal prosecution, is contemplated against any person responsible for the compromise of classified information, DFS will furnish its damage assessment to either OIG or OI.

Losses or Compromise of Classified Information or Sensitive Unclassified Information (C) (continued)

Actions Against Individuals (6) (continued)

Action Involving Criminal Prosecution (c)

When a damage assessment reveals that a violation of criminal law appears to have occurred and a criminal prosecution is contemplated, the agency responsible for the damage assessment will coordinate the contemplated prosecution with the DOJ. OIG or **OI,** depending upon which office has jurisdiction, will coordinate any contemplated prosecution that involves NRC with the DOJ.

Part VI

Prohibitions on Wiretapping and Eavesdropping Devices

This part relates to surreptitious use of wiretapping or eavesdropping devices in conversations or wire transmission without the consent of any of the participants.*

Procurement and Use of Devices (A)

NRC funds must not be used to purchase wiretapping or eavesdropping devices, except as stated below. These devices must not be installed or used for eavesdropping or wiretapping in or on any NRC building, or installation, or on real estate owned or leased by the **U.S.** Government for the use of the NRC, except as authorized by law. See Title III, "Wire Interception and Interception **of** Oral Communications," of the Omnibus Crime Control and Safe Streets Act of 1968 and the Foreign Intelligence Surveillance Act of 1978.

Services Available From the Division of Facilities and Security (B)

Technical Inspection (1)

The NRC Division of Facilities and Security (DFS), Office of Administration, will, on request, provide for technical inspection of facilities or premises in connection with proposed meetings or otherwise to determine the presence of wiretapping or eavesdropping devices.

*For **NRC policies and procedures related to consensual monitoring** or **recording** of **verbal or wire communications, see Management Directive 2.3, "Telecommunications."**

Services Available From the Division of Facilities and Security (B) (continued)

Notification (2)

If any such device or suspected wiretapping or eavesdropping device is discovered as a result of this inspection or otherwise, DFS must be notified immediately by the most secure and rapid means available. No tests or attempts at removal must be made by anyone who discovers the device or by other personnel advised of the existence of the device, except as authorized either by DFS, which will act in coordination with OIG, or the Federal Bureau of Investigation (FBI).

Staff Assistance (3)

DFS will provide staff assistance in determining whether the object is in fact a wiretapping or eavesdropping device and/or in handling the device. Only DFS will procure or possess devices required for such technical inspections or conduct or authorize such inspections.

Actions To Be Taken Upon Discovery of Devices *(C)*

By Individuals (1)

The individual who discovers an actual or suspected eavesdropping or wiretapping device shall take the following actions:

- Maintain silence or normal conversation in the area in which the device is operative in order to conceal the discovery of the device (a)
- Avoid touching or otherwise tampering with the device (b)
- Provide immediate and constant surveillance of the device at all times until relieved by DFS representatives or directed otherwise by the FBI or DFS (This course of action will prevent any touching or tampering with the device or its unauthorized removal.) (c)
- If the discoverer is alone, enlist assistance from the nearest responsible NRC employee, or the nearest responsible NRC contractor employee if a contractor location is involved, to ensure that the device is kept under surveillance while DFS is being contacted (d)

Actions To Be Taken Upon Discovery of Devices (C) (continued)

By Individuals (1) (continued)

- **As** soon as measures have been taken to ensure constant surveillance of the device, notify DFS by the most secure and rapid means available outside the listening area for the device (Notification by telephone is acceptable, provided the device is not located in a telephone closet or in any way connected to telephone wires. If a telephone cannot be used, the nearest security guard should be notified.) (e)

By DFS *(2)*

DFS will notify OIG if any alleged or suspected criminal violations are involved, and OIG will notify appropriate law enforcement authorities.

Classification (3)

Since there are potential national security implications associated with the discovery or use of these devices, all pertinent information must be classified confidential National Security Information until it is reviewed. If NRC authorized classifiers have determined that classified information is not involved, the information must be handled as "Official Use Only." Documents containing classified or Official Use Only information must be marked accordingly.

Advance Notice of Attachment of Any Devices to Telephone or Teletype Lines (D)

EDO Approval (1)

NRC office and division directors and heads of NRC contractor organizations shall obtain the approval of the EDO, in writing, for any physical wiring attachment or inductive coupling to any telephone or teletype line and of any device that has the inherent capability of monitoring or recording messages. In cases involving NRC staff, contractors, or equipment, the Director, DFS; the IG; and the Chief, Technology Infrastructure Branch, Office of the Chief Information Officer, must be notified in advance of the proposed use of this equipment. This notification must take place even if the device is normally used in routine maintenance or operation.

Advance Notice of Attachment of Any Devices to Telephone or Teletype Lines (D) (continued)

Line Compatibility (2)

Any recording equipment attached to telephone or teletype lines must meet line compatibility requirements of the company supplying the lines.

Instructions to NRC and Contractor Personnel (E)

NRC office and division directors shall ensure that NRC and contractor personnel under their jurisdiction are aware of and observe the procedures specified in this part. Similarly, the heads of NRC contractor organizations have the same responsibility regarding their personnel.

Exhibit 1

Certificate of Possession

This is to certify to the best knowledge and belief of _____

_____
(name of contractor, subcontractor, or other party)

that, with the exception of the items listed below, it has returned to authorized representatives of the Nuclear Regulatory Commission (NRC), or disposed of in accordance with NRC security requirements, all classified documents and classified material originated, produced, or received by the company in connection with work performed by it for NRC under _____
_____except _____
(identify contract, subcontract, or other agreement)

(Identify documents and material retained, length of retention, and indicate classification of each item.)

It is understood and agreed that—

(1) The listed items will retain their present classification until downgraded or declassified by NRC and will be safeguarded in accordance with NRC security requirements;

(2) Unauthorized disclosure of classified information is subject to criminal penalties, as provided for, for example, in the Atomic Energy Act of 1954, as amended, and/or the Espionage Act; and

(3) Any unaccounted—for classified documents or classified material or listed items exposed to unauthorized persons will immediately be reported to NRC or the Federal Bureau of Investigation in accordance with NRC security requirements.

Signature _____
For the (name of contractor, subcontractor, or other party to the agreement).

Title _____

Date _____

Exhibit 2

Certificate of Nonpossession

This is to certify to the best knowledge and belief of _____

_____

(name of contractor, subcontractor, or other party)

that it has returned to authorized representatives of the Nuclear Regulatory Commission (NRC), or disposed of in accordance with NRC security requirements, all classified documents and classified material originated, produced, or received in connection with work performed for NRC under-

_____

_____

(identify contract, subcontract, or other agreement)

Signature_____
For the (name **of** contractor, subcontractor, or other party to the agreement)

Title_____

Date_____

Exhibit 3

Standard Form 700, "Security Container Information"

SECURITY CONTAINER INFORMATION

INSTRUCTIONS

1. COMPLETE PART 1 AND PART 2A (ON END OF FLAP)
2. DETACH PART 1 AND ATTACH TO INSIDE OF CONTAINER
3. MARK PARTS 2 AND 2A WITH THE HIGHEST CLASSIFICATION STORED IN THIS CONTAINER.
4. DETACH PART 2A AND INSERT IN ENVELOPE
5. SEE PRIVACY ACT STATEMENT ON REVERSE.

1. AREA OR POST (If required)	2. BUILDING (If required)	3. ROOM NO.
4. ACTIVITY (DIVISION, BRANCH, SECTION OR OFFICE)		5. CONTAINER NO
6. MFG. & TYPE CONTAINER	7. MFG & TYPE LOCK	8. DATE COMBINATION CHANGED
9. NAME AND SIGNATURE OF PERSON MAKING CHANGE		

10. Immediately notify one of the following persons, if this container is found open and unattended.

EMPLOYEE NAME	HOME ADDRESS	HOME PHONE

1. ATTACH TO INSIDE OF CONTAINER

700-101
NSN 7540-01-214-5372

STANDARD FORM 700 (8-85)
Prescribed by GSA/ISOO
32 CFR 2003

WARNING

WHEN COMBINATION ON PART 2A IS ENCLOSED, THIS ENVELOPE MUST BE SAFEGUARDED IN ACCORDANCE WITH APPROPRIATE SECURITY REQUIREMENTS.

DETACH HERE

CONTAINER NUMBER

COMBINATION

_____ turns to the (Right) (Left) stop at _____
_____ turns to the (Right) (Left) stop at _____
_____ turns to the (Right) (Left) stop at _____
_____ turns to the (Right) (Left) stop at _____

WARNING

THIS COW CONTAINS CLASSIFIED INFORMATION WHEN COMBINATION IS ENTERED.

UNCLASSIFIED UPON CHANGE OF COMBINATION

2A INSERT IN ENVELOPE

SF 700 (8-85)
Prescribed by GSA/ISOO
32 CFR 2003

Front Side

Privacy Act Statement

Authority for solicitation of the information is E.O. 12356, National Security Information, August 1, 1982, which requires that security classified material be used, possessed, and stored only under conditions which will prevent access by unauthorized persons or dissemination to unathorized persons. Disclosure of the information is voluntary, The principal purpose of the information is to provide on the inside of the security container the name, home address, and telephone number of employees who have access to the container and are custodians of the material so that they may be alerted if a container is found open during non-duty hours. Routine uses of the information may include the transfer of information to appropriate Federal, State, local, or foreign agencies when relevant to civil, criminal, or regulatory investigations or prosecution; or pursuant to a request of a Federal agency in connection with the hiring or retention of an employee, the issuance of a security clearance, or the investigation of an employee. If the information is not provided, the employee cannot be designated as a custodian of the material.

Reverse Side

Note: When the SF 700 is reissued, all references to **12356** will be updated to reflect EO **12958**

Exhibit 4

Standard Form 702, "Security Container Check Sheet"

SECURITY CONTAINER CHECK SHEET

TO (if required) | THRU (if required)

CERTIFICATION

I CERTIFY, BY MY INITIALS BELOW, THAT I HAVE OPENED, CLOSED OR CHECKED THIS SECURITY CONTAINER IN ACCORDANCE WITH PERTINENT AGENCY REGULATIONS AND OPERATING INSTRUCTIONS.

MONTH/YEAR

DATE	OPENED BY		CLOSED BY		CHECKED BY		GUARD CHECK (if required)	
	INITIALS	TIME	INITIALS	TIME	INITIALS	TIME	INITIALS	TIME

702-101
NSN 7540-01-213-7900

FOLD HERE—REVERSE FOLD FOR FULL USE OF BOTH SIDES—FOLD HERE

SECURITY CONTAINER CHECK SHEET

FROM | ROOM NO. | BUILDING | CONTAINER NO.

CERTIFICATION

I CERTIFY, BY MY INITIALS BELOW, THAT I HAVE OPENED, CLOSED OR CHECKED THIS SECURITY CONTAINER IN ACCORDANCE WITH PERTINENT AGENCY REGULATIONS AND OPERATING INSTRUCTIONS.

MONTH/YEAR

DATE	OPENED BY		CLOSED BY		CHECKED BY		GUARD CHECK (if required)	
	INITIALS	TIME	INITIALS	TIME	INITIALS	TIME	INITIALS	TIME

STANDARD FORM 702 (8-85)
Prescribed by GSA/ISOO
32 CFR 2003

Exhibit 5

Standard Form 312, "Classified Information Nondisclosure Agreement"

CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT

AN **AGREEMENT** BETWEEN AND THE **UNITED STATES**

(Name of Individual – Printed or typed)

1. Intending to be legally bound, 1 hereby accept the obligations contained in this Agreement in consideration of my being granted access to classified information. As used in this Agreement, classified information is marked or unmarked classified information. including oral communications, that is classified under the standards of Executive Order 12356. or under any other Executive order or statute that prohibits the unauthorized disclosure of information in the interest of national security; and unclassified information that meets the standards for classification and is in the process of a classification determination as provided in Sections 1.1 and 1.2(e) of Executive Order 12356, or under any other Executive order or statute that requires protection for such information in the interest of national security. I understand and accept that by being granted access to classified information, special confidence and trust shall be placed in me by the United States Government.

2. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of classified information, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information have been approved for access to it. and that I understand these procedures.

3. I have been advised that the unauthorized disclosure, unauthorized retention, or negligent handling of classified information by me could cause damage or irreparable injury to the United States or could be used to advantage by a foreign nation. I hereby agree that I will never divulge classified information to anyone unless: (a) I have officially verified that the recipient has been properly authorized by the United States Government to receive it; or (b) I have been given prior written notice of authorization from the Cnited States Government Department or Agency (hereinafter Department or Agency) responsible for the classification of the information or last granting me a security clearance that such disclosure is permitted. I understand that if I am uncertain about the classification status of information. I am required to confirm from an authorized official that the information is unclassified before I may disclose it, except to a person as provided in (a) or (b). above. I further understand that I am obligated to comply with laws and regulations that prohibit the unauthorized disclosure of classified information.

4. I have been advised that any breach of this Agreement may result in the termination of any security clearances I hold; removal from any position of special confidence and trust requiring such clearances: or the termination of my employment or other relationships with the Departments or Agencies that granted my security clearance or clearances. In addition, I have been advised that any unauthorized disclosure of classified information by me may constitute a violation, or violations. of United States criminal laws, including rhe provisions of Sections 641. 793, 794. 798. and •952, Title 18, United States Code, 'the provisions of Section 783(b), Title 50, United States Code, and the provisions of the Intelligence Identities Protection Act of 1982. I recognize that nothing in this Agreement constitutes a waiver by the United States of the right to prosecute me for any statutory violation.

5. I hereby assign to the United States Government all royalties, remunerations, and emoluments that have resulted, will result or may result from any disclosure, publication, or revelation of classified information not consistent with the terms of this Agreement.

6. I understand that the Cnited States Government may seek any remedy available to it to enforce this Agreement including. but not limited to. application for a court order prohibiting disclosure of information in breach of this Agreement.

7. I understand that all classified information to which I have access or may obtain access by signing this Agreement is now and will remain the property of. or under the control of the United States Government unless and until otherwise determined by an authorized official or final ruling of a court of law. I agree that I shall return all classified materials which have. or may come into my possession or for which I am responsible because of such access: (a) upon demand by an authorized representative of the United States Government; (b) upon the conclusion of my employment or other relationship with the Department or Agency that last granted me a security clearance or that provided me access to classified information; or (c) upon conclusion of my employment or other relationship that requires access to classified information. If I do not return such materials upon request, I understand that this may be a violation of Section 793. Title 18, United States Code, a United States criminal law.

8. Unless and until I am released in writing by an authorized representative of the United States Government, I understand that all conditions and obligations imposed upon me by this Ageement apply during the time I am granted access to classified information, and at all times thereafter.

9. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions of this Agreement shall remain in full force and effect.

10. These restrictions are consistent with and do not supersede, conflict with or otherwise alter the employee obligations, rights or liabilities created by Executive Order 12356; Section 7211 of Title 5, United States Code (governing disclosures to Congress); Section 1034 of Title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the military); Section 2302(b)(8) of Title 5, United States Code, as amended by the Whistleblower Protection Act (governing disclosures of illegality. waste, fraud, abuse or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 U.S.C. 421 et seq.) (governing disclosures that could expose confidential Government agents), and the statutes which protect against disclosure that may compromise the national security. including Sections 641, 793. 794, 798. and 952 of Title 18, United States Code, and Section 4(b) of the Subversive Activities Act of 1950 (50 U.S.C. Section 783(b)). The definitions. requirements, obligations, rights, sanctions and liabilities created by said Executive Order and listed statutes are incorporated into this Agreemenr and are controlling.

(Continue on reverse.)

NSN 7540-01-280-5499
Previous edition not usable.

312-102

STANDARD FORM 312 (REV. 1–91)
Prescribed by GSA/ISOO
32 CFR 2003, E.O. 12356

Exhibit 5 (continued)

SIGNATURE	DATE	SOCIAL SECURITY NUMBER (See Notice below)

WITNESS		ACCEPTANCE	
THE EXECUTION OF THIS AGREEMENT WAS WITNESSED BY THE UNDERSIGNED.		THE UNDERSIGNED ACCEPTED THIS AGREEMENT ON BEHALF OF THE UNITED STATES GOVERNMENT.	
SIGNATURE	DATE	SIGNATURE	DATR
NAME AND ADDRESS (Type or print)		NAME AND ADDRESS (Type or print)	

SIGNATURE OF EMPLOYEE	DATE

NAME OF WITNESS (Type or print)	SIGNATURE OF WITNESS

Note: When the SF 312 is reissued all references to EO 12356 will be updated to reflect EO 12958

U.S. NUCLEAR REGULATORY COMMISSION

DIRECTIVE TRANSMITTAL

TN: DT–99–11

To:	NRC Management Directives Custodians
Subject:	Transmittal of Directive 12.2, "NRC Classified Information Security Program"
Purpose:	Directive and Handbook 12.2 have been revised to reflect changes as a result of Executive Order 12958, "Classified National Security Information." Minor changes concerning responsibilities and authorities were made, and new procedures were established for managing an NRC classified information security program. Revision bars have not been used to indicate changes because the handbook was entirely reorganized.
Office and Division of Origin:	Office of Administration
Contact:	Wayne Burnside, (301) 415-2211
Date Approved:	May 13, 1993 **(Revised: April 27, 1999)**
Directive:	12.2, "NRC Classified Information Security Program"
Availability:	Rules and Directives Branch Office of Administration David L. Meyer (301) 415–7162 or Jeannette P. Kiminas (301) 415–7086

NRC Classified Information Security Program

Directive 12.2

Contents

Policy 1

Objective 1

Organizational Responsibilities and Delegations of Authority 1

- Chairman 1
- The Commission 2
- Secretary of the Commission 2
- Executive Director for Operations (EDO) 2
- Deputy Executive Director for Management Services (DEDM) 2
- Director, Office of Administration (ADM) 3
- Director, Office of International Programs (OIP) 3
- Office Directors and Regional Administrators 4
- Director, Division of Facilities and Security (DFS), ADM 4

Applicability 5

Handbook 5

Exceptions or Deviations 5

References 5

NRC Classified Information Security Program
Directive 12.2

Policy
(12.2–01)

All U.S. Nuclear Regulatory Commission personnel responsible for safeguarding classified information (National Security Information, Restricted Data, and Formerly Restricted Data) and activities involving this information shall adhere to the procedures in this directive and handbook.

Objective
(12.2–02)

To ensure that classified information is handled appropriately and is protected from unauthorized disclosure in accordance with pertinent laws, Executive orders, other management directives, and applicable directives of other Federal agencies and organizations.

Organizational Responsibilities and Delegations of Authority
(12.2–03)

Chairman
(031)

- Designates NRC personnel authorized original Top Secret classification authority. This authority may not be delegated. (a)
- Designates, if required, NRC and other personnel authorized original Secret or Confidential classification authority. This authority may be delegated. (b)

The Commission
(032)

- Approves the waiver of requirements normally applicable in furnishing classified information to foreign governments. (a)
- Acts on appeals for denial of information requested under the mandatory review procedures of Executive Order 12958 when the request involves information generated by the Chairman, the Commissioners, or Commission-level offices. (b)
- Reviews and approves classification guides that could affect NRC major policy decisions before these guides are published. (c)
- As delegated by the Chairman, has original Top Secret classification authority. (d)

Secretary of the Commission
(033)

Ensures proper control and accountability over all classified documents containing National Security Council Information.

Executive Director for Operations (EDO)
(034)

- As delegated by the Chairman, has original Top Secret classification authority. (a)
- As assigned by the Chairman, responsible for delegating original classification authority at the Secret and Confidential levels to NRC and NRC contractor employees. (b)

Deputy Executive Director for Management Services (DEDM)
(035)

- Actively oversees implementation of Executive Order 12958 by NRC, NRC contractors, NRC licensees, and licensee-related organizations. (a)
- Designates original classifying authority at Secret and Confidential levels to NRC and NRC contractor personnel, except for those officials designated in Commission-level offices. (b)

Deputy Executive Director for Management Services (DEDM)
(035) (continued)

- Approves classification guides, except those requiring Commission approval. (d)
- Issues and maintains guidelines for systematic review for declassification of 25-year-old National Security Information under NRC jurisdiction and 40-year-old classified foreign government information in NRC custody for use by the Archivist of the United States and, upon approval, by any agency holding the information. (e)
- Approves the designation of NRC personnel authorized to declassify or downgrade National Security Information. (f)
- Approves plans for the protection of classified information in an emergency. (g)
- Acts on appeals for denial of information requested under the mandatory review procedures of Executive Order 12958 when the request involves information generated by offices and regions reporting to the EDO. (h)

Director, Office of International Programs (OIP)
(036)

- Determines if furnishing classified information to international organizations will result in a net advantage to the national security interests of the United States. (a)
- Assists in the development of classified information exchange agreements with foreign countries or international organizations. (b)

Director, Office of Administration (ADM)
(037)

Provides overall NRC security program guidance and direction and ensures that NRC's security program is effectively and efficiently carried out by the NRC Division of Facilities and Security (DFS), ADM.

Office Directors and Regional Administrators
(038)

- Ensure that NRC employees and NRC contractor personnel under their jurisdiction are cognizant of and comply with the provisions of this directive and handbook. (a)
- Advise DFS of any existing or proposed classified activities in organizations under their jurisdiction. Report any significant change or termination of classified activities to DFS for review of associated contracts, subcontracts, or similar actions. (b)
- Furnish security plans to DFS, as appropriate. (c)
- Advise DFS of any information that indicates noncompliance with this directive and handbook or is otherwise pertinent to the proper protection of classified interests and information. (d)
- Support and implement NRC's security classification program. (e)
- Control and safeguard classified information under their jurisdiction in accordance with this directive and handbook. (f)
- Request exceptions to or deviations from this directive and handbook, as required. (g)

Director, Division of Facilities and Security (DFS), ADM
(039)

- Plans, develops, establishes, and administers policies, standards, and procedures for the NRC classified information security program, including management of the security classification program. (a)
- Administers the security aspects of the disclosure of National Security Information to foreign governments and international organizations. (b)
- Renders foreign ownership, control, or influence (FOCI) determinations and facility security clearances. (c)

Applicability
(12.2–04)

The policy and guidance in this directive and handbook apply to all NRC employees, NRC contractors as a condition of a contract or purchase order, and NRC consultants as a condition of the consultant agreements. However, they do not affect Commission rules and regulations contained in the *Code of Federal Regulations* that are applicable to NRC licensees and others.

Handbook
(12.2–05)

Handbook 12.2 contains guidelines for the preparation, distribution, accountability, classification, and safeguarding of classified information.

Exceptions or Deviations
(12.2–06)

DFS may grant exceptions to or deviations from this directive and handbook except in those areas in which the responsibility or authority is vested solely with the Commission and the DEDM and is nondelegable or for matters specifically required by law, Executive order, or directive to be referred to other management officials.

References
(12.2–07)

Atomic Energy Act of 1954, as amended (42 U.S.C. 2011, et seq.).

Code of Federal Regulations—

10 CFR Part 2, "Rules of Practice for Domestic Licensing Proceedings."

10 CFR Part 9, "Public Records."

10 CFR Part 25, "Access Authorization for Licensee Personnel."

10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities."

10 CFR Part 51, "Environmental Protection Regulations for Domestic Licensing and Related Regulatory Functions."

10 CFR Part 70, "Domestic Licensing of Special Nuclear Material."

10 CFR Part 71, "Packaging and Transportation of Radioactive Material."

References

(12.2–07) (continued)

10 CFR Part 95, "Security Facility Approval and Safeguarding of National Security Information and Restricted Data."

"Crimes and Criminal Proceedings," Title 18, *United States Code*.

Director of Central Intelligence Directives, including No. 1/7-1, "Security Controls on the Dissemination of Intelligence Information," June 30, 1998.

Energy Reorganization Act of 1974, as amended (42 U.S.C. 5801, et seq.).

Executive Order 12333, "United States Intelligence Activities," December 4, 1981.

— 12829, "National Industrial Security Program," as amended, January 8, 1993.

— 12958, "Classified National Security Information," and related directives of the Information Security Oversight Office, National Archives and Records Administration, April 20, 1995.

— 12968, "Access to Classified Information, August 2, 1995.

"Freedom of Information" (5 U.S.C. 552).

National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations, December 17, 1969.

National Security Decision Directive 2 (NSDD-2), "National Security Council Structure," January 12, 1982.

— 19 (NSDD-19), "Protection of Classified National Security Council and Intelligence Information," January 12, 1982.

National Security Decision Memorandum 119 (NSDM-119), "Disclosure of Classified Military Information to Foreign Governments and International Organizations," July 20, 1971.

NRC Management Directive—

3.1, "Freedom of Information Act."

3.2, "Privacy Act."

5.5, "Public Affairs Program."

12.1, "NRC Facility Security Program."

12.3, "NRC Personnel Security Program."

References
(12.2–07) (continued)

12.4, "NRC Telecommunications Systems Security Program."

12.5, "NRC Automated Information Systems Security Program."

12.6, "NRC Sensitive Unclassified Information Security Program."

NUREG-0910, Rev. 2, "NRC Comprehensive Records Disposition Schedule" (February 1998).

"Privacy Act" (5 U.S.C. 552a).

NRC Classified Information Security Program

Handbook 12.2

Contents

Part I

Protection and Control of Classified Information 1

Scope (A) 1
Classification (B) 1
Responsibilities To Protect Classified Information (1) 1
Classification of Protected Information (2) 6
Marking Classified Documents (3) 9
Change of Classification and Marking (4) 13
Declassification of National Security Information (5) 18
Deletion of Classified Information From Documents (6) 21
Markings for Specific Types of Classified Information (7) 22
Record Classification Actions (RCA) System (8) 26
Control of Secret and Confidential Documents (C) 27
Cover Sheets (1) 27
Assurances Required Before Transmission of Classified Information (2) 27
Means of Transmission of Secret Documents (3) 28
Means of Transmission of Confidential Documents (4) 29
Electronically Transmitted Classified Messages (5) 30
Transmission of Documents From Other Agencies (6) 31
Preparation of Secret and Confidential Documents for Transmission (7) 31
Classified Documents From Other Agencies (8) 33
Destruction of Secret and Confidential Documents (9) 34
Loss or Possible Compromise of Classified Information (10) 34
Classification Guides (D) 35
Types of Guides (1) 35
Contents of Guides (2) 36
Approval of Guides (3) 36
Review of Guides (4) 36
Dissemination of Guides (5) 36
Content of Guides (6) 36
Classification Appraisals (E) 37
Frequency of Appraisals (1) 37
Reports (2) 37
Foreign Ownership, Control, or Influence (FOCI) (F) 38

Contents (continued)

Part II

Protection and Control of Foreign Intelligence Information 41

Scope (A) 41
Access to Foreign Intelligence Information (B) 41
Authorization for Access (1) 41
Emergency Authorization for FII Access (2) 42
Security Education and Awareness Briefing (3) 42
Termination of Access (4) 42
Contractors and Consultants (5) 43
Control of Documents (C) 43
Markings (1) 43
Reproduction (2) 44
Release to Foreign Governments, Foreign Nationals, or Other Than U.S. Citizens (3) 45
Release to Other Government Agencies (4) 45
Transmission (5) 45
Accountability (6) 47
Classified Meetings or Presentations (7) 48
Storage (8) 48
Destruction (9) 49
Unauthorized Disclosure of Classified FII (D) 49
Classification, Declassification, or Downgrading (E) 49

Part III

Special Handling of Classified Information 50

Control of Top Secret Documents (A) 50
Top Secret Control Officers (1) 50
Accountability Control Files (2) 51
Assignment of a Control Number to Documents From Other Agencies (3) ... 52
Physical Inventory (4) 53
Reproduction of Top Secret Documents (5) 54
Reproduction of Top Secret Documents From Other Agencies (6) 54
Transmission of Top Secret Documents (7) 55

Contents (continued)

Part III (continued)

Receipts (8) 55
Destruction of Top Secret Documents (9) 55
Naval Nuclear Propulsion Information (B) 56
National Security Council Information (NSCI) (C) 57
Responsibilities (1) 57
Access Lists (2) 57
Requirements (3) 57
Transfer of Classified Information to Foreign Governments and International Organizations (D) 60
Authorities (1) 60
Criteria (2) 61
Responsibilities (3) 62
Internal Procedures (4) 64
Access Lists (5) 68
Sanctions (6) 69
Classified Conferences (E) 69
Conferences and Symposia (1) 69
Publication or Release of Documents (2) 70
Review of Documents (3) 70
Review of Documents Submitted by Uncleared Authors (4) 70
Review of Documents Submitted by Formerly Cleared Persons or by Authors With Active Clearances (5) 71
Transporting Classified Material via Commercial Airlines (F) 71

Exhibits

1 Required Markings for Classified Documents 74
2 Declassification Markings 75
3 Subject or Title Marking and Portion-Marking 76
4 Upgrading, Downgrading, and Transclassification Markings 77
5 Deleting Classified Information From Classified Documents 78

Contents (continued)

Exhibits (continued)

6 Required Markings for Unclassified Transmittal Document 79
7 Required Markings for Classified Transmittal Document 80
8 Required Markings for Envelopes or Wrappers 81

Part I

Protection and Control of Classified Information

Scope (A)

The procedures for classification and control of information, to ensure a uniform system for safeguarding classified information, are discussed below. These procedures implement the provisions of the Atomic Energy Act (AEA) of 1954, as amended; the Energy Reorganization Act of 1974, as amended; Executive orders (e.g., EO 12958, "Classified National Security Information"), and other directives (e.g., directives of the Information Security Oversight Office (ISOO), National Archives and Records Administration).

Classification (B)

Classification is a means of identifying information concerning the national defense and foreign relations of the United States that requires protection against disclosure to unauthorized persons. It enables access to the information to be restricted to properly cleared and authorized persons who require access to perform official duties.

Responsibilities To Protect Classified Information (1)

Classification Determinations (a)

Classification determinations regarding NRC information must be made solely by NRC authorized classifiers, including NRC contractors who have been delegated that authority. Authorized classifiers are delegated either original or derivative classification authority. (i)

An authorized classifier with original classification authority may determine, on the basis of his or her knowledge, authority, and expertise—(ii)

Classification (B) (continued)

Responsibilities To Protect Classified Information (1) (continued)

- Whether or not National Security Information requires classification (*a*)
- The classification level necessary to protect National Security Information in those cases in which the information is not already covered by classification guidance or when the classification level has not otherwise been previously determined (*b*)

An authorized classifier with derivative classification authority only may classify information on the basis of classification determinations made by an original classification authority, a source document, or other classification guidance (e.g., a classification guide, a bulletin, or a notice). Also, as recognized by EO 12958, the AEA constitutes the authority for classification of Restricted Data and Formerly Restricted Data, and because AEA classifies this information at its inception, all these classification determinations are derivative. Each official with original classification authority also possesses derivative classification authority. (iii)

Delegation of Classification Authority (b)

A Presidential Order of October 17, 1995, designates the Chairman of the NRC as a Top Secret original classification authority under EO 12958, Section 1.4. As authorized, the Chairman has delegated original classification authority to the four Commissioners, Executive Director for Operations (EDO), and Deputy Executive Director for Management Services (DEDM). The Chairman also has assigned the EDO and DEDM responsibility for delegating original classification authority at the Secret and Confidential levels to NRC and NRC contractor personnel. The responsibility for delegating derivative classification authority to NRC personnel, NRC contractor personnel, and other personnel has been assigned by the DEDM to the Director, Division of Facilities and Security (DFS), Office of Administration (ADM). (i)

The appropriate office director or regional administrator shall submit all requests for classification authority or changes to existing authority (original or derivative), in writing, to the Director, DFS. These requests must include—(ii)

- Names and positions of the individuals for whom authority is sought (*a*)

Classification (B) (continued)

Responsibilities To Protect Classified Information (1) (continued)

- Level of classification authority requested (*b*)
- Justification for this request, including a description of the type of information that will require classification and the expected frequency with which this authority will be exercised (*c*)

Upon receipt of the written request for classification authority, the Director, DFS, will evaluate the request and take the necessary action to approve or disapprove it, or have the DEDM approve or disapprove a request for original classification authority. (iii)

Authorized Classifier Training (c)

The Information Security Branch (INFOSEC) conducts classifier training when an individual is delegated classification authority.

Responsibilities of Authorized Classifiers (d)

Each person possessing original or derivative classification authority is accountable for his or her classification actions. Unnecessary classification, over classification, and under classification must be avoided. (i)

Authorized original classifiers may make classification determinations only up to the level for which they have been delegated authority. Authorized derivative classifiers may classify only that information that is—(ii)

- Identified in a classification guide (*a*)
- Derived from a source document (*b*)
- Assigned a classification determination by an authorized original classifier (*c*)

In any case, it is the responsibility of the authorized classifier (iii)

- To decide whether information requires classification (*a*)
- To determine the level of classification to be applied to this information (*b*)
- To verify, insofar as practical, that classification guidance as well as the classification level is current before assigning a derivative classification (*c*)

Classification (B) (continued)

Responsibilities To Protect Classified Information (1) (continued)

Any authorized classifier may determine that information not previously classified is unclassified. This determination is different from a declassification determination concerning currently classified information. The authorized classifier may use as guidance the information contained in: (iv)

- Classification guides or other guidance approved for use (see Section (D) of this part) (*a*)
- Previously declassified information (*b*)
- Documents already determined to be unclassified (*c*)

When an authorized classifier is in doubt as to whether information is classifiable, the interpretation of a classification guide topic or which topic applies, or the proper level of classification, the matter should be promptly referred to the next higher classification authority or to DFS for a determination. In instances in which there is reasonable doubt about the need to classify information or the appropriate classification level, the following actions must be taken: (v)

- If the need to classify information is in question, the information must be safeguarded at least as if it were Confidential, pending a determination about its classification. If it is determined that the information should be classified, the information must be marked and protected accordingly. (*a*)
- If the appropriate classification level is in question, the information must be safeguarded at the highest level of classification at issue and with the most restrictive category that may be assigned to it, pending a determination about its classification level and the applicable category. When the classification level and category have been determined, the information must be marked and protected accordingly. (*b*)

If there is significant doubt about the need to classify information it shall not be classified. (vi)

In all cases, a determination must be made within 30 days. (vii)

Authorized classifiers also are responsible for ensuring that information they determine is classified is marked and protected in accordance with the provisions of this handbook. (viii)

Classification (B) (continued)

Responsibilities To Protect Classified Information (1) (continued)

Responsibilities of Originators (d)

If the originator of information is not an authorized classifier but believes that this information may require classification, he or she shall refer the information to an authorized classifier for a decision. If the originator is certain that the information is unclassified, he or she need not refer the information to an authorized classifier but shall handle it accordingly. (i)

If the originator of classified information is an authorized classifier, he or she shall classify the information in accordance with the responsibilities identified in Section (B)(1) of this part. (ii)

Classification Challenges (e)

Persons who are in authorized possession of classified National Security Information and who in good faith believe that the information's classification level is too high a level for its content (over classification) or too low for its content (under classification) are expected to challenge the classification status of that information. (i)

Persons who wish to challenge classification status shall—(ii)

- Refer the document or information to the originator or to an authorized NRC classifier for review. The authorized classifier shall review the document and render a written classification decision to the holder of the information. (*a*)
- In the event of a question regarding classification review, the holder of the information or the authorized classifier shall consult INFOSEC, DFS, for assistance. (*b*)
- Persons who challenge classification decisions have the right to appeal the decision to the Interagency Security Classification Appeals Panel. INFOSEC, DFS, should be contacted in the event of an appeal. (*c*)
- Persons seeking to challenge the classification of information will not be subject to retribution. (*d*)

Classification (B) (continued)

Responsibilities To Protect Classified Information (1) (continued)

Limitations on Classification (f)

Information must not be classified to conceal violations of the law, inefficiency, or administrative error; to prevent embarrassment to a person, an organization, or an agency; to restrain competition; or to prevent or delay the release of information that does not require protection in the interest of national security. (i)

Basic scientific research information not clearly related to the national security may not be classified. (ii)

Classification of Protected Information (2)

Classification Process (a)

Classification is the process of identifying information that NRC needs to protect in the interest of the national defense and foreign relations. This information must be designated as "National Security Information," "Restricted Data," or "Formerly Restricted Data." Classification also involves determining the level and duration of classification and ensuring that information is properly marked. Among other considerations, a determination of whether or not information is classified must be made on the basis of the information that may be revealed by study, analysis, and/or observation, or use and/or by association with other information, including that which is known to be in the public domain. Classification determinations also must be made on the assumption that any person who has access to the information is highly qualified in the particular field and thoroughly familiar with the data that have been treated as unclassified in the general subject area.

Types of Information That May Be Classified in Each Category (b)

The three categories of classified information are "National Security Information," "Restricted Data," and "Formerly Restricted Data."

National Security Information (i)

Information may not be considered for classification as National Security Information unless it concerns—(*a*)

- Military plans, weapons systems, or operations (*1*)

Classification (B) (continued)

Classification of Protected Information (2) (continued)

- Foreign government information (*2*)
- Intelligence activities (including special activities) or intelligence sources or methods or cryptology (*3*)
- Foreign relations or foreign activities of the United States, including confidential sources (*4*)
- Scientific, technological, or economic matters relating to national security (*5*)
- United States Government programs for safeguarding nuclear materials or facilities (*6*)
- The vulnerabilities or capabilities of systems, installations, projects, or plans relating to national security (*7*)

Certain information that would otherwise be unclassified may require classification when combined or associated with other classified or unclassified information. Classification on this basis must be supported by a written explanation that must be maintained with the file or record copy of the information. (*b*)

National Security Information classified in accordance with Section (B)(2)(b)(i) of this part must not be automatically declassified as a result of any unofficial publication or inadvertent or unauthorized disclosure of identical or similar information. (*c*)

Restricted Data and Formerly Restricted Data (ii)

AEA is the basis for the determination that all Restricted Data and Formerly Restricted Data are classified. AEA Section II defines Restricted Data and Section 142 establishes the basis for the concept of Formerly Restricted Data. All Restricted Data and Formerly Restricted Data classification actions are derived from the AEA. Current classification guidance conveys the types of information that must be designated as Restricted Data and Formerly Restricted Data and the classification level that must be assigned to the information. This classification guidance may be obtained from INFOSEC, DFS. (a)

Classification (B) (continued)

Classification of Protected Information (2) (continued)

Levels of Classification (c)

The three levels of classification for the protection of both National Security Information and Restricted Data are "Top Secret," "Secret," and "Confidential." Only these three classification designators may be used to identify the level of classification assigned to information.

Sensitivity of the Information (i)

Sensitivity of the information involved is the basis for assigning the level of classification. As the sensitivity of the information increases, so does the level of classification and protection afforded the information.

Classification Authority (ii)

The classification authority for National Security Information is the authorized original classifier, a classification guide, or a source document. The classification authority for Restricted Data or Formerly Restricted Data is AEA, as refined by classification guides.

Duration of Classification (iii)

The duration of classification is the length of time the information must remain classified. For original classifications, National Security Information must be classified in accordance with EO 12958. At the time of original classification, the original classifier shall attempt to identify a specific date or event for declassification that is less than 10 years from the date of the original classification. If the original classifier cannot determine a date or event for declassification, the information shall be marked for declassification 10 years from the date of original classification.

Declassification Exemptions (iv)

National Security Information may be exempted from declassification within 10 years if the information could reasonably be expected to cause damage to the national security and it qualifies for exemption under EO 12958, Section 1.6(d). Normally, exemption from declassification may not exceed 25 years.

Classification (B) (continued)

Classification of Protected Information (2) (continued)

Classification Extensions (v)

If National Security Information cannot be declassified upon the specific date or event for declassification set at the time of classification, an original classification authority may extend the duration of classification for additional periods not to exceed 10 years at a time. For information of permanent historical value, successive periods of classification extension may not exceed 25 years, as it is then automatically declassified under EO 12958, Section 3.4.

Information Classified Under Previous Executive Orders (vi)

National Security Information marked "Originating Agency's Determination Required" (OADR) under previous Executive orders may be declassified if the information is declassifiable under EO 12958. The information may be remarked to establish a duration of classification consistent with the requirements of EO 12958, or if the information is of permanent historical value, it may remain classified for 25 years from the date of original classification when it is automatically declassified in accordance with EO 12958, Section 3.4.

Restricted Data and Formerly Restricted Data Exemption (vii)

Restricted Data and Formerly Restricted Data are exempt from automatic declassification. AEA Sections 141 and 142 set forth the policy regarding review and declassification of Restricted Data and transfer of information from the Restricted Data category to the Formerly Restricted Data status. See Section (B)(4) for declassification of National Security Information, Restricted Data, and Formerly Restricted Data.

Marking Classified Documents (3)

In the preparation of classified documents, the highest overall classification must be placed at the top and bottom of the front cover (if any), the title page (if any), the first page, and the outside of the back cover (if any). The appropriate classification level markings (e.g., "TOP SECRET," "SECRET," or "CONFIDENTIAL"), or the marking "UNCLASSIFIED" if a page contains no classified information, must be placed at the top and bottom of each page. If so desired, the highest overall classification level of the entire document may be

Classification (B) (continued)

Marking Classified Documents (3) (continued)

placed at the top and bottom of each page. However, for Restricted Data, classifiers shall ensure that documents containing Restricted Data and Formerly Restricted Data are clearly marked at the top and bottom of each interior page with the overall classification level and category. In all cases, the following markings must be placed on the face of all classified documents, the front cover, the title page, or the first page of each classified document (See Exhibit 1 of this handbook).

Category of Classified Information (a)

The category markings for Restricted Data or Formerly Restricted Data must be placed on the lower left side of the document. The category marking for National Security Information need not be placed on the document.

Classification Markings for National Security Information (b)

Information classified under EO 12958 must show the name or personal identifier, position title of the original classifier, the specific reason for classification as identified in EO 12958, the declassification instructions indicating the decision for the duration of the classification. An example of the classification marking follows. (i)

Classified By: David Smith, Chief, ABC Branch

Reason: (Cite reason from EO 12958, Section 1.5)

Declassify On: (Date or event for declassification not to exceed 10 years from the original classification decision)

If a classifier determines that National Security Information is exempt from 10-year declassification, the classifier must cite one of the exemption categories identified in EO 12958, Section 1.6(d), on the "Declassify On" line. (ii)

If it is determined that National Security Information must remain classified longer than 10 years, the original classifier may extend the declassification date for periods not to exceed 10 years at a time and to a maximum of 25 years. For example—(iii)

Declassify On: (Classification extended on October 1, 1996 until October 1, 2006 by Chief, XYZ Branch.)

Classification (B) (continued)

Marking Classified Documents (3) (continued)

Classification Markings for Restricted Data (c)

Restricted Data will not have the same classification markings as National Security Information. Documents classified as "Restricted Data" will have the following category marking stamped in the lower left of the first page of the document: (i)

> This documents contains Restricted Data as defined in the Atomic Energy Act of 1954. Unauthorized disclosure subject to Administrative and Criminal sanctions.

In addition, the source and classifier of Restricted Data must be identified by the following marking:

Classified By: Classification Guide ABC

Derivative Classifier: _____
(Name and Title)

Declassification Markings (d)

Only authorized declassifiers appointed by DFS may declassify National Security Information. Restricted Data may be declassified by persons appointed by the Department of Energy (DOE). (i)

The following marking must be placed on the front of all National Security Information documents that have been declassified (see Exhibit 2 of this handbook): (ii)

> This document has been declassified under the provisions of Executive Order 12958, dated April 17, 1995.
>
> By Authority of _____
> (Declassification Authority)
>
> Date of Declassification _____

Classification Authority (e)

The classification authority for National Security Information is the authorized classier, the classification guide, or the source document. If a document is classified on the basis of more that one source document or classification guide, the phrase "Multiple Sources" must be cited as

Classification (B) (continued)

Marking Classified Documents (3) (continued)

the classification authority. The date of declassification marking on multiple source documents will reflect the source that provides the longest period of classification. (i)

The classification authority for Restricted Data and Formerly Restricted Data is the authorized derivative classifier. Original classification authority for Restricted Data lies with DOE under AEA. NRC may not make original classification decisions for Restricted Data. (ii)

Portion Marking (f)

Each section, part, paragraph, or similar portion of a classified document shall be marked to show the highest level of its classification, or that the portion is unclassified (see Exhibit 3 of this handbook). Portions of documents shall be marked in a manner that eliminates doubt as to which of its portions contain or reveal classified information. Each portion of a document containing National Security Information must be marked. Documents containing Restricted Data and Formerly Restricted Data may have portions of the text marked. (i)

- To mark portions of the text in a classified document, one of the following appropriate classification abbreviations is placed parenthetically immediately before or after the text (e.g., titles, graphics, and subjects) it governs. (*a*)

  (TS) for Top Secret

  (S) for Secret

  (C) for Confidential

  (U) for Unclassified

- If a document contains a combination of categories of classified information, the appropriate classification must be coupled with the following appropriate category and placed parenthetically immediately before or after the text it governs. (*b*)

  (RD) for Restricted Data

  (FRD) for Formerly Restricted Data

Classification (B) (continued)

Marking Classified Documents (3) (continued)

(NSI) for National Security Information

For example: (CRD), (SRD), or (TSNSI)

- If it is not practical to use a parenthetical designation, the document must contain a statement identifying the information that is classified and the level and category of classification. If all portions of a document are classified at the same level and category, a statement to this effect is sufficient without marking or specifying each item. (*c*)

ISOO may waive the portion-marking requirement for specific classes of information upon a written determination either that there will be minimal circulation of the specified information in documented form and minimal potential usage of these documents or their information as a source for derivative classification determinations or that there is some other basis to conclude that the potential benefits of portion-marking are clearly outweighed by the increased administrative burden. Requests for waivers should be addressed to the Director, DFS, who will evaluate and make the appropriate recommendation to ISOO. (ii)

Change of Classification and Marking (4)

Upgrading (a)

A notice that a document containing National Security Information was mistakenly issued as unclassified or was mistakenly declassified must be classified and marked at an appropriate level. A notice that a document containing Restricted Data was issued as unclassified or was mistakenly declassified must be classified and marked at least "CRD" (Confidential Restricted Data). If the notice contains information requiring a higher classification or a more restrictive category, the notice must be marked accordingly (see Exhibit 1 of this handbook for placement of markings). (i)

Classification (B) (continued)

Change of Classification and Marking (4) (continued)

The notice of classification or upgrading must identify the appropriate document as fully as possible, stating—(ii)

- Title, subject, or a brief description of the document (*a*)
- Document number, if any (*b*)
- Author of the document (*c*)
- Date of the document (*d*)
- Person authorizing the classification or upgrading (*e*)
- Portions of the document to be classified or upgraded, if appropriate (*f*)
- All markings, including portion-markings, to be placed on the document (*g*)

The notice will be distributed to all regional administrators and office directors; the Secretary of the Commission; the Director, Information Management Division, Office of the Chief Information Officer; the Chief, Physical Security Branch, DFS; and all known holders of the document, as determined by DFS. (iii)

The fact that a document was mistakenly declassified or issued as unclassified must not be disclosed over unsecured telephone lines. (iv)

After all copies of the document have been properly classified or destroyed, the notice must be declassified, unless the content of the notice is classified (see Section (B)(5) of this part for declassification). (v)

A notice that a classified document has been upgraded to a higher classification may be unclassified, provided no classified information is included in the notice. (vi)

Upon receipt of a notice of classification or upgrading, the document is to be marked as indicated by the notice of classification. (vii)

Classification (B) (continued)

Change of Classification and Marking (4) (continued)

Remarking requires marking out the existing classification markings at the top and bottom of each page, and all identified portion-marking designators. The new upgraded classification portion-marking designators must then be inserted next to the marked-out designators. If the document is bound, only the classification on the outside of the front cover, the title page, the first and the last page of text, and the outside of the back cover need be marked out and replaced with the upgraded classification. Additionally, the following statement is to be placed on the face of the document, the cover, the title page, or the first page of text. (See Exhibit 4.) (viii)

Classification changed to: (insert new level)

By authority of: (person authorizing change)

By: (signature of person making change)

Date: (date of change)

Downgrading (b)

National Security Information may be downgraded by the authorized classifier who originally classified the information (if he or she is still serving in the same position), by the originator's successor, or by a supervisor of either who possesses original classification authority. Also, the Director, DFS, and the Chief, INFOSEC, have been delegated downgrading authority. (i)

DFS should be consulted for downgrading instructions. Restricted Data and Formerly Restricted Data may only be downgraded in accordance with approved classification guidance (e.g., classification guides or bulletins). (ii)

Upon the determination by an authorized individual that a document can be downgraded, a notice of downgrading must be issued and the individual authorizing the downgrading of a Secret document shall notify all known holders of the document. (iii)

Classification (B) (continued)

Change of Classification and Marking (4) (continued)

The downgrading notice must identify the document as fully as possible, stating—(iv)

- Title, subject, or a brief description of the document (*a*)
- Document number (*b*)
- Originator of the document (*c*)
- Date of the document (*d*)
- Person authorizing the downgrading (*e*)
- New classification level that will be assigned to the document (*f*)
- Effective date of the change (*g*)
- If appropriate, the portions of the document to be downgraded (*h*)

If the recipient of a downgrading notice has forwarded the document to another custodian, the downgrading notice must also be forwarded to the other custodian. (v)

Upon reaching the assigned automatic downgrading date or event or upon receipt of a downgrading notice, the person responsible for downgrading the document shall mark out the existing classification at the top and bottom of each page and all identified portion-marking designators. The new downgraded classification and portion-marking designators must then be placed next to the marked-out designators. If the document is bound, only the classification on the front cover, the title page, the first and the last page of text, and the outside back cover need be marked out and replaced with the new downgraded classification. (vii)

Additionally, the statement below is to be placed on the face of the document, the cover, the title page, or the first page of the text of any document being downgraded by a notice. The statement is not required on documents downgraded in accordance with automatic downgrading instructions. (viii)

Classification (B) (continued)

Change of Classification and Marking (4) (continued)

Classification changed to: (insert new level)

By authority of: (person authorizing change)

By: (signature of person making change)

Date: (date of change)

Restricted Data and Formerly Restricted Data are exempt from automatic downgrading. National Security Information may be subject to automatic downgrading at some date before declassification if the authorized original classifier determines that the sensitivity of the document will decrease upon the occurrence of a specific event or with the passage of time. When automatic downgrading instructions are placed on a document at the time of origin (that is, the marking "DOWNGRADE TO _____ON _____" is placed under the classification authority notation on the lower right side of the document (see Exhibit 4). The document will be downgraded on the assigned date or upon the occurrence of the designated event, with no notice to holders required. (ix)

The custodian shall either downgrade his or her copy of the document on or after the date or event specified or ensure that the document will be downgraded when it is withdrawn from the files. If the custodian believes that the downgrading is inappropriate, he or she shall refer the matter to the Director, DFS. (x)

Transclassification (c)

"Transclassification" is the transfer of information from the Restricted Data category to the Formerly Restricted Data category. All transclassification actions must be in accordance with AEA Sections 142 d. and e. and must take place only upon written notification of this change by the Director, DFS. Contact DFS when necessary to transclassify information. (i)

Upon receipt of a transclassification notice, the person responsible for the transclassification shall cross out the existing Restricted Data marking and insert the "Formerly Restricted Data" marking below or beside the marked-out classification (see Exhibit 4). Additionally, the following statement must be placed on the face of the document, the cover, the title page, or the first page of text. (ii)

Classification (B) (continued)

Change of Classification and Marking (4) (continued)

Category changed to: (insert new category)

By authority of: (person authorizing change)

By: (signature of person making change)

Date: (Date of change)

Declassification of National Security Information (5)

Authorities (a)

National Security Information may be declassified by the authorized classifier who originally classified the information (if he or she is still serving in the same position), the originator's successor, a supervisor of either who possesses original classification authority, or a designated declassification authority such as the Director, DFS, and the Chief, INFOSEC. (i)

Restricted Data and Formerly Restricted Data can only be declassified in accordance with AEA Section 142. Any proposed declassification actions for these categories of classified information must be forwarded to the Director, DFS, who will coordinate the matter with other affected agencies, as necessary. (ii)

Automatic Declassification (b)

National Security Information of permanent historical value that is 25 years old or older is subject to automatic declassification unless the classification has been extended or the information is exempt from declassification under EO 12958. (i)

Information may be exempted from automatic declassification if that information would (ii)

- Reveal the identity of an individual who is a confidential source or reveal information regarding intelligence sources and methods or individual intelligence sources, the disclosure of which would clearly damage national security (*a*)
- Assist in the development or use of weapons of mass destruction (*b*)
- Impair U.S. cryptologic systems or activities (*c*)

Classification (B) (continued)

Declassification of National Security Information (5) (continued)

- Reveal actual U.S. military war plans that remain in effect (*d*)
- Clearly and demonstrably impair U.S. foreign relations or clearly impair the U.S. Government's ability to protect the President, Vice President, or other officials (*e*)
- Clearly and demonstrably impair national preparedness plans (*f*)
- Violate a statute, treaty, or international agreement (*g*)

Exemptions of information from automatic declassification must be approved by appointed declassification authorities. (iii)

Declassification Reviews (c)

Any declassification review of documents that may contain information from other agencies or that may be of direct interest to other agencies will be coordinated with the affected agencies by Director, DFS.

Standard Declassification Reviews (i)

Standard declassification reviews result from a request within NRC, from NRC contractors or other organizations associated with an NRC program or a request from other Government agencies to review documents for declassification. In these cases, a request for declassification of National Security Information must be forwarded to the authorized classifier responsible for the original classification, his or her successor, a supervisor of either with the required declassification authority, or the Director, DFS. Restricted Data and Formerly Restricted Data will be declassified in accordance with the provisions of Section (B)(2)(c)(vii) of this part.

Freedom of Information Act (FOIA) or Privacy Act (PA) Declassification Reviews (ii)

Declassification reviews and other actions involving review of classified information in accordance with FOIA or PA must be conducted in accordance with the provisions of this part and Management Directive (MD) 3.1, "Freedom of Information Act." (a)

The Director, DFS, will attempt to resolve any disagreements on the releasability of information contained in classified documents that are requested under the FOIA or the PA. (b)

Classification (B) (continued)

Declassification of National Security Information (5) (continued)

If the NRC receives an FOIA or PA request for records in its possession that were classified by another agency, the NRC will forward the request and a copy of the records requested to that agency for processing and may, after consultation with the originating agency, inform the requester of the referral. In those instances in which the other agency does not want its identity disclosed or the existence or nonexistence of the requested information is itself classifiable, the response to the requester will comply with these restraints. (c)

Mandatory Review for Declassification (iii)

NRC information classified under EO 12958 or earlier Executive orders is subject to a review for declassification under provisions of EO 12958, Section 3.6. All such declassification reviews will be conducted in accordance with the "NRC Mandatory Review for Declassification Procedures," published in the Federal Register on November 5, 1996, and available from DFS upon request.

Systematic Review for Declassification (iv)

NRC information classified under EO 12958 or earlier orders is subject to a review for declassification under the provisions of EO 12958, Section 3.5. All such declassification reviews will be conducted in accordance with the NRC systematic review guidelines, which are available from DFS upon request.

Notice of Declassification (v)

Upon the determination by an authorized individual that a document can be declassified, the following actions must be taken, as appropriate:

- **Top Secret Documents.** The individual authorizing the declassification of a Top Secret document shall notify the Director, DFS, who in turn shall notify custodians of all copies. (*a*)
- **Secret or Confidential Documents.** The individual authorizing the declassification of a Secret document shall send a notice of declassification to all known holders of the document. An information copy of this notice also must be sent to the Director, DFS. (*b*)

Classification (B) (continued)

Declassification of National Security Information (5) (continued)

- **Contents of the Notice.** Declassification notices must identify the document as fully as possible, stating the title, subject, or a brief description of the document; the document number, if any; the originator of the document; the date of the document; the person authorizing the declassification; and the effective date of the declassification. These notices will normally be unclassified unless some unusual circumstances require the inclusion of classified information. (*c*)

- **Forwarding of the Notice.** If the recipient of a declassification notice has forwarded the document to another custodian, the declassification notice also must be forwarded to the other custodian. However, for documents declassified under the automatic declassification provision of EO 12958, Section 3.4, a notification is not necessary because these documents are official record copies that were released to the Public Document Room after declassification. (*d*)

Deletion of Classified Information From Documents (6)

Deleting classified information from documents involves the physical removal of classified information so as to produce an unclassified version of the original document (see Exhibit 5). (a)

An authorized classifier from the office that originated the document shall identify the classified information to be removed from the document. DFS will be available for consultation to ensure that all classified information is identified. (b)

After identification of the classified information, the responsible person shall ensure that the classified information is removed from the document and cross out the category and classification authority markings that appear on the front cover, title page or first page, and the classification at the top and bottom of each page. If the document is bound, only the classification on the front cover, title page, first and the last page of text, and the outside back cover need be crossed out. (c)

The following statement is to be placed on the face of the document, front cover, title page, or the first page of text of all documents in which the classified information has been deleted: (d)

Classification (B) (continued)

Deletion of Classified Information From Documents (6) (continued)

The classified information has been removed from this document.

This copy of the document is UNCLASSIFIED.

By Authority of: (person authorizing deletion)

By: (signature of person deleting the classified information and the date of removal)

Markings for Specific Types of Classified Information (7)

Transmittal Documents (a)

Unclassified Transmittal Documents (i)

The classification marking on the first page of an unclassified transmittal document must be equivalent to the highest level of classification being transmitted. Other pages of the transmittal document may have the same classification marking or may be marked "UNCLASSIFIED." (a)

Additionally, if the information is Restricted Data, the lower left side of the first page of the transmittal document must be marked to identify it as transmitting Restricted Data. The lower right side of the first page of the transmittal must be marked: "When separated from the attachments this document is "UNCLASSIFIED." The transmittal document is not classified and does not required marking when the Restricted Data is not attached. (b)

See Exhibit 6 for proper markings and placement of markings on unclassified transmittal documents. (c)

Classified Transmittal Documents (ii)

Classified transmittal documents must be classified and marked as required by their content in accordance with Sections (B)(2) and (3) of this part. However, in some instances, classified transmittal documents may require the following additional markings (see Exhibit 7):

Classification (B) (continued)

Markings for Specific Types of Classified Information (7) (continued)

- If the transmittal document is of a lower classification than any document being transmitted, the classification on the first page of the transmittal document must be equivalent to the highest level of classification being transmitted. Other pages of the transmittal document must be marked to reflect the information contained therein. (*a*)

- The lower right side of the first page of the transmittal document must be marked to identify the classification of the transmittal document when it is removed from the attachments. (*b*)

- If the category of classified information identified for the transmittal document is less restrictive than that of any document being transmitted, the lower left side of the transmittal document also must be marked to reflect the most restrictive category of classified information being transmitted. (*c*)

- The recipient of a transmittal document may downgrade or declassify his or her copy of the transmittal document without further authorization if the transmittal document is removed from the attachments and is to remain permanently separated from them. The downgrading and declassification marking requirements of Sections (B)(4)(b) and B(5)(c)(v) of this part, respectively, must be followed. (*d*)

Compilations (iii)

A compilation composed of several existing documents must be treated as a new document and classified and marked in accordance with Section (B)(2) and (3) of this part. Classification for the new document must be supported by a written explanation that, at a minimum, must be maintained with the file or referenced on the record copy of the information.

Files or Folders Containing Classified Documents (iv)

Files or folders containing classified documents must be marked on the outside front and back with a classification equivalent to the highest level of classification contained therein or, if warranted by assemblage or compilation, a higher classification level.

Classification (B) (continued)

Markings for Specific Types of Classified Information (7) (continued)

Drafts and Working Copies (b)

Drafts and working copies of documents that contain classified information must be marked with the appropriate classification level and Restricted Data category marking if the draft contains Restricted Data, in accordance with Section (B)(3)(c) of this part. (i)

Other markings (e.g., classification authority, duration, portion-marking, and documentation) are not required unless the document will be distributed outside the preparing office or maintained for file, record, reference, background, or historical purposes. In these instances, the document must be classified and entered into the automated record classification actions system in accordance with Section (B)(8) of this part. (ii)

Top Secret documents must be documented in accordance with Part III(A) of this handbook, except that the series designator must be assigned as "Draft 1," "Draft 2," and so forth or "Working Copy 1," "Working Copy 2," and so forth in lieu of an alphabet letter. (iii)

Reproduction and Dissemination Limitations (c)

If the originator of a classified document determines that the document must be subject to special reproduction and/or dissemination limitations, the following statement must be placed on the lower left side of the face of the document, the cover, the title page, or the first page of text: (i)

> Reproduction or further dissemination requires approval of (insert title of authorizing official). See Section (C) of this part for procedures for reproducing Top Secret, Secret, and Confidential documents.

Foreign Government Information (d)

Information received from foreign governments must either retain its original classification designation or be assigned a United States classification level that will ensure a degree of protection at least equivalent to that required by the entity that furnished the information. In addition, such documents must be identified by placing the "FOREIGN GOVERNMENT INFORMATION" marking on the lower right side of the face of the document, the cover, the title page, or the first page of text. (i)

Classification (B) (continued)

Markings for Specific Types of Classified Information (7) (continued)

Documents originated by NRC that contain foreign government information must be marked in accordance with Section (B)(3) of this part. These documents also must be identified with the "FOREIGN GOVERNMENT INFORMATION" marking. Any paragraphs that contain foreign government information must be so identified by placing the designator "FGI" in parentheses before or after the text it governs. (ii)

The "FOREIGN GOVERNMENT INFORMATION" marking and the "FGI" portion-marking designator must not be used if the fact that the information is from a foreign government must be concealed. In these instances, the information must be marked in accordance with Section (B)(3) of this part, as if it were wholly of United States origin. (iii)

Word Processor Disks (e)

Word processor disks that contain classified information must be marked as follows: (i)

- The manufacturer's label on the disk must be marked with a classification level equivalent to the highest level classification contained on the disk. (*a*)
- The disk file folder or box must be marked in accordance with Section (B)(7)(a)(iv) of this part. (*b*)
- If a label is placed on the disk or file folder to list or identify the individual documents contained on the disk, the appropriate portion-marking designators identified in Section (B)(3)(f) of this part, must be parenthetically placed after the name of each document. (*c*)

NRC personnel who mark word processor disks should use the pre-printed labels available for that purpose. DFS should be contacted for information regarding other media containing classified information (e.g., video tapes, photographs, charts, maps, recordings, or microfilm). (ii)

Classification (B) (continued)

Markings for Specific Types of Classified Information (7) (continued)

Translations (f)

Translations of United States classified information into a language other than English must be marked in accordance with this part. Translations also must be marked to show the United States as the country of origin and with the foreign language equivalent markings (see Section (B)(7)(d) of this part for documents received from foreign countries).

Record Classification Actions (RCA) System (8)

The RCA system ensures that current and accurate information is available for use by NRC in fulfilling its reporting responsibility to ISOO and provides traceability of classification, downgrading, and declassification actions during appraisals, inspections, or audits. (a)

The RCA system is available in automated form via the authorized classifier's personal computer, which should be used in lieu of paper copies of NRC Form 790, "Classification Record." Alternatively, a completed NRC Form 790, may be completed and submitted to DFS by the authorized original or derivative classifier authorizing a classification, downgrading, or declassification action, excluding automatic downgrading or declassification. The authorized classifier submits the original and one copy of NRC Form 790 to DFS and retains one copy for his or her files. DFS will monitor all data index input and maintain the system's records. (b)

DFS is responsible for preparing specific reports on classification actions that are taken on the basis of information provided by the RCA system, and for submitting these reports to ISOO on predetermined dates. The RCA system enables DFS to verify proper classification actions during appraisals, inspections, or audits in order to effectively administer the NRC Security Program. (c)

Control of Secret and Confidential Documents (C)

Cover Sheets (1)

A "SECRET" cover sheet, Standard Form 704, or a "CONFIDENTIAL" cover sheet, Standard Form 705 must be placed on the face of each copy of a document classified as Secret or Confidential upon preparation, or upon receipt from outside sources if no form is attached. The cover sheet must remain on the copy whether the copy is held by NRC, NRC contractors or subcontractors, or transmitted to other destinations. The cover sheet need not be retained on Secret or Confidential documents in the file but must be placed on these documents when they are withdrawn from the file and must remain with the documents until the documents are destroyed. Upon destruction of the documents, the cover sheet may be removed, and depending on its condition, reused.

Assurances Required Before Transmission of Classified Information (2)

Before the transmission of classified information, the sender shall ensure that the recipient needs the information to perform official duties, is authorized to receive the information, possesses the appropriate access authorization, and has approved storage facilities for safeguarding the information. The sender may obtain assurance of this information from DFS or the recipient's cognizant security office. (a)

Before delivering hand-carried classified documents to the addressee or the authorized recipient, the individual delivering the documents shall require positive identification of the addressee or the recipient. (b)

The removal of classified documents from approved facilities to private residences or other unapproved places for work purposes is prohibited. Also, leaving classified documents unattended in motels or hotels during official travel is prohibited. (c)

All classified documents, when not in the possession of authorized individuals, must be stored only in approved facilities (see MD 12.1 for storage of classified documents). (d)

Bulk quantities of classified documents must be handled in accordance with instructions obtained from the Director, DFS. (e)

Control of Secret and Confidential Documents (C) (continued)

Means of Transmission of Secret Documents (3)

Persons hand-carrying Secret documents shall keep the documents continuously in their possession until the documents are stored in an approved facility. (a)

Secret documents, transmitted internally within facilities, must be hand-delivered by persons authorized access to the information or transmitted by approved internal mail service. (b)

Secret documents transmitted externally to outside facilities must be delivered by—(c)

- Methods approved for the transmission of Top Secret documents (i)
- An authorized person hand-carrying the information (Authority for NRC or NRC contractor employees to hand-carry Secret documents outside a facility must be obtained from the Director, DFS) (ii)
- U.S. Postal Service registered mail or U.S. Postal Service express mail within and between the 50 States, the District of Columbia, and Puerto Rico (iii)
- A cleared commercial carrier or a cleared commercial messenger service engaged in intracity/local delivery of classified mail (iv)
- A commercial delivery company approved by DFS that provides nationwide, overnight service with computer tracing and reporting features (Such companies do not need a security clearance.) (v)
- U.S. Postal Service registered mail through Army, Navy, or Air Force postal service facilities (This method must have prior approval from the Director, DFS, and assurance that the information will not pass out of control of United States citizens or through a foreign postal system. This method may be used to transmit Secret documents to and from the United States Government or its contractor employees or members of the Armed Forces in a foreign country.) (vi)

Control of Secret and Confidential Documents (C) (continued)

Means of Transmission of Secret Documents (3) (continued)

- Department of State diplomatic pouch (Documents may be transmitted to United States Government employees, contractor employees, or members of the Armed Forces in a foreign country by use of the Department of State diplomatic pouch. This method must be approved by the Director, DFS, before it is used. The approval may be granted for individual transmissions or on a blanket basis.) (vii)

- An authorized person hand-carrying Secret documents to and from foreign countries (The approval of the Director, DFS, must be obtained before hand-carrying Secret documents to or from a foreign country. Arrangements must be made to preclude the necessity for customs examination of the documents. Employees transporting Secret documents must use vehicles or aircraft owned by the U.S. Government or its contractors, ships of the U.S. Navy, U.S. naval ships manned by the civil service, and ships of U.S. registry. This method of transmission may be permitted only when other means set forth above are impractical and it is necessary to perform official duties.) (viii)

Means of Transmission of Confidential Documents (4)

Persons hand-carrying Confidential documents shall keep the documents continuously in their possession until the documents are stored in an approved facility or are turned over to a designated recipient. (a)

Confidential documents, transmitted internally within facilities, must be hand-delivered by persons authorized access to the information or transmitted by an approved internal mail service. (b)

Confidential documents, transmitted externally to outside facilities, must be delivered by—(c)

- Methods approved for the transmission of Secret documents (i)

- U.S. Postal Service certified or express mail within and between the 50 States, the District of Columbia, Puerto Rico, and U.S. territories or possessions (ii)

Control of Secret and Confidential Documents (C) (continued)

Electronically Transmitted Classified Messages (5)

Classified messages must be transmitted only by electronic means approved by DFS. Procedures applicable to handling classified messages within approved communications centers are set forth in MD 12.4, "NRC Telecommunications Systems Security Program." (a)

All paper copies of electrically transmitted classified messages must be marked in accordance with Sections (B)(2) and (3) of this part. (b)

The originator of a classified message shall be considered the classifier. Accordingly, a "Classified by" line is not required on messages in these instances. If the originator is not the classifier, the words "Classified by" and the identity of the classifier must be indicated before the text. (c)

Portion-marking must be used to identify the classified and unclassified portions of the message. Text must be portion-marked in accordance with Section (B)(3)(f) of this part. (d)

The last line of text of a classified message containing National Security Information must show the date or event for automatic declassification or the appropriate exemption marking. (e)

Upon receipt of a classified message, the transmitting communications center person shall—(f)

- Review the message to determine that required security classification markings have been applied to the form and the message. (i)
- Encrypt, transmit, or otherwise dispatch the message in accordance with MD 2.3, "Telecommunications," and MD 12.4. (ii)
- Return to the originating office all messages containing notations requesting their return. (iii)
- Destroy all copies of classified messages in the center's possession 90 days after transmission unless a longer period is approved by a regional administrator or the Director, DFS. (iv)
- Maintain records of the destruction of all Secret messages. (v)

Control of Secret and Confidential Documents (C) (continued)

Electronically Transmitted Classified Messages (5) (continued)

Upon receipt of a classified message, the receiving communications center person must—(g)

- Receive, decrypt, and edit the message as prescribed by MD 2.3 and add the security markings in accordance with Sections (B)(3) and (4) of this part. (i)
- Ensure that the message is given to the addressee. (ii)
- Destroy all copies of classified messages in the center's possession 90 days after receipt unless a longer period is approved by a regional administrator or the Director, DFS. (iii)
- Maintain records of the destruction of all Secret messages. (iv)

Transmission of Documents From Other Agencies (6)

Classified documents originated by other agencies must not be disseminated outside NRC or NRC contractor offices without the written consent of the originating agency. (a)

Upon receipt of written consent, the transmission must be handled in accordance with Sections (C)(3), (4), or (5) of this part. (b)

A copy of the written consent for transmission of classified documents from other agencies must be forwarded to the Director, DFS, and maintained with the record copy of the document. (c)

Preparation of Secret and Confidential Documents for Transmission (7)

Secret and Confidential documents transported by authorized individuals within an approved building or facility need only be placed in a cover that conceals the document when it may be observed by unauthorized individuals. However, documents transported outside an approved building or facility to another agency via any means must be handled in accordance with this section.

Preparation of Receipts (a)

The sender shall complete NRC Form 253, "Messenger/Courier Receipt." Copies of this form must be distributed according to the instructions on the form. (i)

Control of Secret and Confidential Documents (C) (continued)

Preparation of Secret and Confidential Documents for Transmission (7) (continued)

Individual forms must be used for each addressee. (ii)

More than one document may be included on the forms if the same sender and addressee are involved. (iii)

Verification, Signature, and Return of Receipts (b)

NRC Form 126, "Classified Document Receipt," must be used for outside transmission of classified information. For transmission of classified information within NRC facilities an NRC Form 126 is not required.

Envelopes and Wrappers (c)

Classified documents must be enclosed in two opaque envelopes or wrappers for transmission or delivery outside an approved building or facility. The envelopes will be marked as shown in Exhibit 8.

Inner Envelope or Wrapper (i)

The inner envelope or wrapper must be addressed to the person for whom the document is intended. The address approved for classified mail must be used. The classification must be placed at the top and bottom on the front and back of the inner envelope or wrapper. (a)

If documents bearing different classification levels are transmitted in the same envelope or wrapper, the marking must be that of the highest classified document, or a higher one if warranted because of assemblage of the documents. (b)

The marking "Restricted Data" or "Formerly Restricted Data" must appear on the front and back of each inner envelope or wrapper, if appropriate. (c)

Outer Envelope or Wrapper (ii)

The outer envelope or wrapper must be adequately sealed and addressed in the ordinary manner with no indication on the envelope that it contains a classified document. (a)

The address for classified mail of the intended recipient must be used. Under no circumstances should the name of the intended recipient appear on the outer envelope. (b)

Control of Secret and Confidential Documents (C) (continued)

Preparation of Secret and Confidential Documents for Transmission (7) (continued)

Evidence of Tampering (iii)

If the envelope or wrapper used in the transmission of classified Documents indicates any evidence of tampering, the recipient shall preserve the envelope or wrapper as received and immediately notify DFS, those personnel responsible for the security functions in the recipient's office, and the NRC Office of the Inspector General.

Classified Documents From Other Agencies (8)

Safeguards To Be Afforded (a)

Documents from other agencies must be safeguarded with at least those precautions prescribed for documents of the same classification level originated by NRC.

Third Agency Rule (b)

The "Third Agency Rule" provides that "classified information originating in one agency may not be disseminated outside any other agency to which it has been made available without the consent of the originating agency" (see EO 12958). No exceptions to this rule are permitted unless coordinated, in advance, with the Director, DFS.

Registered Documents (c)

On occasion, NRC or NRC contractors will receive documents originated by personnel of the Department of Defense that are numbered and contain the notation on the cover "Registered Document," "Serial Document," or a similar designation. In these cases, NRC employees or NRC contractor personnel shall comply with the inventory and reporting requirements established by the originating agency. Personnel are to consult DFS regarding these requirements.

Responsibility for Change of Classification and Declassification (d)

Classified documents originated by other agencies must be upgraded, downgraded, transclassified, or declassified only upon written consent of the originating agency, unless the document is marked to indicate automatic downgrading or declassification.

Control of Secret and Confidential Documents (C) (continued)

Classified Documents From Other Agencies (8) (continued)

Documents Received Without Required Markings (e)

When NRC receives reports or other correspondence from another agency without the required classification level, category of classified information, or other markings, DFS will apply the appropriate markings and will notify the other agency of such action.

Destruction of Secret and Confidential Documents (9)

Responsibilities (a)

Secret and Confidential documents must be destroyed by the custodian or other authorized individuals.

Method of Destruction (b)

Secret and Confidential classified waste (except for Foreign Intelligence Information; see Part II of this handbook) must be disposed of by shredding with an approved shredder or other specified method or by placing the waste in the classified waste receptacles located throughout NRC buildings. (i)

Classified microfilm and microfiche must be destroyed by burning or by a chemical process to ensure complete destruction or total eradication of the images recorded. (ii)

Before acquisition of a shredder to destroy classified documents, the shredder must be approved by DFS in accordance with the procedures set forth in MD 13. 1, "Personal Property Management." (iii)

Contractors shall use classified waste disposal methods approved by DFS. (iv)

Loss or Possible Compromise of Classified Information (10)

DFS shall be advised if personnel responsible for the security function are unable to resolve discrepancies or if there is any indication that classified documents are unaccounted for. (a)

Any person who has knowledge of the loss or possible compromise of classified information shall immediately report (within 1 hour) the circumstances to DFS. Upon receipt of this report, DFS shall initiate an inquiry into the matter. (b)

Control of Secret and Confidential Documents (C) (continued)

Loss or Possible Compromise of Classified Information (10) (continued)

If the information was originated by another agency, DFS shall notify officials of the agency involved so that a damage assessment may be conducted and appropriate measures taken to negate or minimize any adverse effect. (c)

DFS also will determine the cause of the loss or compromise, place responsibility, and take corrective measures to prevent a similar occurrence. Appropriate administrative, disciplinary, or legal action will be taken if warranted. (d)

Classification Guides (D)

Classification guides are required under EO 12958, Section 2.3, for the classification of National Security Information. There are also classification guides for Restricted Data and Formerly Restricted Data.

Types of Guides (1)

Within NRC, classification guides are grouped in the following types

Program Classification Guides (a)

These guides apply classification policy to a particular aspect of the NRC program through specific topical items. Guides frequently involve the mission of more than one office. The Director, DFS, is responsible for the issuance and revision of these guides. A program guide establishes an authoritative frame of reference within which more detailed local classification guides may be prepared. (i)

In conjunction with appropriate offices and regions, DFS determines that a program classification guide is needed to implement policy in a field of work or that an existing program guide requires revision. DFS will coordinate the subsequent preparation of these guides with appropriate NRC offices and regions and with other agencies, as required. (ii)

Local Classification Guides (b)

These guides are established on the basis of program classification guides. They provide detailed guidance for the classification of programs or segments of programs that are carried out wholly under the jurisdiction of, or that are unique to, a single organization.

Classification Guides (D) (continued)

Contents of Guides (2)

Classification guides must—

- Indicate the information to be protected using categorization to the extent necessary to readily and uniformly identify relevant areas (a)
- Indicate the classification levels (e.g., Top Secret, Secret, or Confidential) and the categories of information (e.g., National Security Information, Restricted Data, or Formerly Restricted Data) (b)
- Indicate the duration of the classification, and appropriate declassification instructions (c)

Approval of Guides (3)

The Deputy Executive Director for Management Services (DEDM) will approve each program classification guide in writing. Any program guide that could affect major NRC policy decisions will be forwarded to the Commission for review before being issued. (a)

Each local classification guide must be submitted to the Director, DFS, for approval before it is issued. (b)

Review of Guides (4)

Each classification guide will be kept current and reviewed at least every 5 years. DFS will maintain a list of all NRC classification guides in use and will schedule reviews according to the dates the guides were issued.

Dissemination of Guides (5)

DFS shall distribute classification guides as widely as necessary to ensure the proper and uniform derivative classification of information.

Content of Guides (6)

As a minimum, classification guides should—

- Identify the subject matter of the classification guide, the original classification authority by name and position, and the agency point-of-contact for questions (a)

Classification Guides (D) (continued)

Content of Guides (6) (continued)

- Provide the date of issuance or last review (b)
- State precisely the elements of information to be protected, which classification level applies to each element of information, and specify the elements that are unclassified (c)
- State special handling caveats (d)
- Prescribe declassification instruction or the exemption category (e)
- Specify the exemption category identified in EO 12958 Section 1.6(d) (f)
- State a concise reason for classification (g)

Classification Appraisals (E)

Classification appraisals are conducted by DFS to review the classification, downgrading, and declassification practices and procedures of NRC, NRC contractors, and other organizations to determine the accuracy and uniformity of interpretation and implementation of NRC policy and standards. DFS has survey and appraisal guidance for the standard format used for classification appraisals.

Frequency of Appraisals (1)

The Director, DFS, determines the appraisal intervals for all headquarters offices, regional offices, contractors, and other organizations. Circumstances may indicate a need for yearly appraisals of some offices, regions, contractors, and other organizations, whereas other appraisals could be at longer intervals.

Reports (2)

A written report must be prepared after each appraisal that clearly delineates the classification practices of the organization appraised. (a)

Classification Appraisals (E) (continued)

Reports (2) (continued)

Normally, the appraisal results will be discussed with management personnel of the appraised organization before completion of the final report. When this practice is considered inappropriate, the discussion will be held with the director of the headquarters office, the regional administrator, the contractor, or the management staff of any other organization concerned. (b)

Copies of the findings and recommendations from the appraisal will be furnished to the regional office, the headquarters office, the contractor, or other appraised organization. A copy of the appraisal report will be furnished to the Director, DFS. (c)

NRC headquarters offices, regional offices, contractors, or other organizations will take prompt action to ensure that necessary corrective measures are introduced on the basis of recommendations contained in the report. DFS must be provided written confirmation that the necessary corrective measures have been taken. (d)

Foreign Ownership, Control, or Influence (FOCI) (F)

The National Industrial Security Program Operating Manual (NISPOM) implements the provisions of EO 12829. A company is considered to be under FOCI whenever a foreign interest has the power, direct or indirect, whether or not exercised, and whether or not exercisable through the ownership of the U.S. company's securities, by contractual arrangements or otherwise, to direct or decide matters affecting the management or operations of that company in a manner that may result in unauthorized access to classified or may adversely affect the performance of classified information contracts. Upon receiving indication that a potential NRC contractor requires access to classified information (as evidenced by designation under block 5 of the NRC Form 187), the Division of Contracts and Property Management shall forward the NRC Form 187 and Statement of Work to DFS for assessment to determine whether or not a reasonable basis exists for concluding that a compromise or unauthorized disclosure of classified information may occur. (1)

Foreign Ownership, Control, or Influence (FOCI) (F) (continued)

A U.S. company determined to be under FOCI is not eligible for facility clearance (FCL). If a company already has an FCL, the FCL shall be suspended or revoked unless security measures are taken to remove the possibility of unauthorized access to classified information. (2)

DFS will consider the following factors to determine whether a company is under FOCI, its eligibility for an FCL, and the protective measures required. (3)

- Foreign intelligence threat (a)
- Risk of unauthorized technology transfer (b)
- Type and sensitivity of the information requiring protection (c)
- Nature and extent of FOCI to include whether a foreign person occupies a controlling or dominant minority position; source of FOCI to include identification of immediate and ultimate parent organizations (d)
- Record of compliance with pertinent U.S. laws, regulations, and contracts (e)
- Nature of bilateral and multilateral security and information exchange agreement (f)

DFS may require contractors being assessed for FOCI to provide information concerning—(4)

- Direct or indirect ownership of 5 percent or more of applicant company's voting stock by a foreign person (a)
- Direct or indirect ownership of 25 percent or more of any class of the applicant company's non-voting stock by a foreign person (b)
- Management positions, such as directors, officers, or executive personnel of the applicant company held by other than U.S. citizens (c)
- Power of a foreign person to control the election, appointment, or tenure of directors, officers, or executive personnel of the applicant company and the power to control decisions or activities of the applicant company (d)

Foreign Ownership, Control, or Influence (FOCI) (F) (continued)

- Contracts, agreements, understandings, or arrangements between the applicant company and foreign person (e)
- Details of loan arrangements between company and a foreign person if the company's overall debt to equity ratio is 40:60 or greater; and details of any significant portion of the company's financial obligations that are subject to the ability of a foreign person to demand repayment (f)
- Total revenues or net income in excess of 5 percent from a single foreign person or in excess of 30 percent from foreign persons in the aggregate (g)
- Ten percent or more of any class of voting stock in "nominee shares" or in "street name" or in some other method that does not disclose the beneficial owner (h)
- Interlocking directors with foreign persons and any officer or management official of the applicant company who is also employed by a foreign person (i)
- Any other factor that indicates or demonstrates a capability on the part of foreign persons to control or influence the operations or management of the applicant company (j)
- Ownership of 10 percent or more of any foreign interest (k)

If an applicant company provides information that would indicate FOCI concerns, DFS shall review the case to determine the relative significance of the information relative to the factors listed under paragraphs (3) and (4) above, the extent to which FOCI could result in unauthorized access to classified information and the type of actions necessary to negate the effects of FOCI to an acceptable level. However, if DFS determines a company is under FOCI, DFS shall suspend the FCL (5)

Part II

Protection and Control of Foreign Intelligence Information

Scope (A)

Foreign Intelligence Information (FII) is information relating to the capabilities, intentions, and activities of foreign powers, organizations, or persons, but not including counterintelligence information, as it relates to international terrorist activities. Procedures for the protection of FII, other than Sensitive Compartmented Information (SCI), to which NRC personnel have access, are discussed below. Procedures for the control and management of SCI are available through the Division of Facilities and Security (DFS), Office of Administration, to personnel authorized access to that category of information.

Access to Foreign Intelligence Information (B)

Authorization for Access (1)

NRC personnel may have access to FII if they meet the following conditions: (a)

- A requirement for FII in the performance of their official duties (i.e., a need to know) (i)
- Proper access authorization (i.e., security clearance) (ii)
- Identified by the Commissioners, an office director, regional administrator, or DFS as having a need to know in the performance of his or her duties (iii)
- Attendance at, or reading of, the FII Security Education and Awareness Briefing (iv)

Access to Foreign Intelligence Information (B) (continued)

Authorization for Access (1) (continued)

DFS annually requests a need-to-know listing from NRC organizations and maintains a complete listing for the NRC. When office or personnel conditions change, a new or amended listing should be submitted to DFS within 30 days. (b)

Emergency Authorization for FII Access (2)

Emergency situations may arise in which immediate additions are necessary to an office's need-to-know listing. In these cases, NRC officials currently on the list may grant immediate access after confirming the NRC employee has the proper clearance. This emergency authorization does not include NRC contractors or consultants or other persons not employed by NRC. The Director, DFS, is authorized to grant immediate one-time access to FII for persons who have a need to know and who are cleared at the appropriate level.

Security Education and Awareness Briefing (3)

NRC personnel are required to attend an FII Security Education and Awareness Briefing, which is produced and presented by DFS to specifically address the controls and handling required for this particular category of classified information. Copies of this briefing will be provided to each NRC region so that regional personnel may satisfy this requirement by reading the FII briefing material. Attendance will be recorded on NRC Form 268, "Security Education/Awareness Briefing Attendance."

Termination of Access (4)

The Information Security Branch (INFOSEC), DFS, should be notified by the office director or regional administrator when an employee—

- No longer requires FII in the performance of his or her official duties (a)
- Announces his or her intention to leave NRC or his or her employment is terminated (b)
- Security considerations dictate the termination of need-to-know access by the Director, DFS (c)

Access to Foreign Intelligence Information (B) (continued)

Contractors and Consultants (5)

Contractors or consultants, or other persons not employed by NRC, are not authorized access to FII in the NRC. In the event it becomes necessary for a person to have access to FII in the performance of his or her duties, a written request delineating the official need for the information and specific information required, will be made to the Director, DFS. Approval may only be granted by the originating agency of the FII and the appropriate cognizant security authority on a case-by-case basis.

Control of Documents (C)

Markings (1)

Each classified document containing FII originated by NRC personnel will be marked on the front cover, or on its face if there is no front cover, with the classification and other control markings (caveats) prescribed by DCID 1/7, "Security Controls on the Dissemination of Intelligence Information," dated June 30, 1998, and this part. (a)

Control markings will be transferred to any other format or media when the information is converted to written, oral, or visual presentations. Consent must be obtained from the originating agency or department for any exceptions to the restrictions established by the control markings. Consent, if granted, applies only to the specific purpose agreed to by the originating agency or department. Recipients of FII are bound by the original control markings on the information. (b)

Questions regarding any control markings that are used on documents containing FII should be referred to DFS. One or more of the following control markings may appear on FII documents. (c)

- The marking, "DISSEMINATION AND EXTRACTION OF INFORMATION CONTROLLED BY ORIGINATOR," (ORCON) or (OC), may be used only on classified intelligence that clearly identifies or would reasonably permit ready identification of intelligence sources or methods that are particularly susceptible to countermeasures that would nullify or measurably reduce their effectiveness. It is used to enable the originator to maintain continuing knowledge and supervision of distribution of the

Control of Documents (C) (continued)

Markings (1) (continued)

intelligence beyond its original dissemination. This control marking may not be used when access to the intelligence information will reasonably be protected by use of its classification markings (i.e., Confidential, Secret, or Top Secret) or by use of any other control markings specified herein or in other DCIDs. (i)

- The marking, "CAUTION-PROPRIETARY INFORMATION INVOLVED" (PROPIN or PR), is used, with or without a security classification, to identify information provided by a commercial firm or a private source under an express or implied understanding that the information will be protected as a proprietary trade secret or proprietary data believed to have actual or potential value. This marking precludes dissemination to contractors irrespective of their status to, or within, the U.S. Government without the authorization of the originator of the intelligence and provider of the information. (ii)
- The marking, "NOT RELEASABLE TO FOREIGN NATIONAL" (NOFORN or NF), is used to identify intelligence that an originator has determined falls under the criteria of DCID 5/6, "Intelligence Which May Not Be Disclosed or Released," and may not be provided in any form to foreign governments, international organizations, coalition partners, foreign nationals, or immigrant aliens without originator approval. (iii)
- The marking, "AUTHORIZED FOR RELEASE TO...(name of country(ies)/international organization)" (REL TO), is used when a limited exception to the marking requirements in Section 9.4 may be authorized to release the information beyond US recipients. This control marking is authorized only when the originator has an intelligence sharing arrangement or relationship with a foreign government approved in accordance with policies and procedures of the Director, Control Intelligence (DCI), that permits the release of the specific intelligence information to the foreign government, but to no other in any form without originator consent. (iv)

Reproduction (2)

NRC personnel or other personnel associated with the NRC program may not reproduce classified documents containing FII without written authorization from the Director, DFS, to ensure application of appropriate markings and compliance with NRC accountability requirements.

Control of Documents (C) (continued)

Release to Foreign Governments, Foreign Nationals, or Other Than U.S. Citizens (3)

NRC personnel, may not release classified documents containing FII, although they may not contain additional control markings, to foreign governments, foreign nationals, or other than U.S. citizens. A formal intelligence sharing arrangement or relationship with a foreign government and approved in accordance with DCI policies and procedures is required for such releases.

Release to Other Government Agencies (4)

The "Third Agency Rule" provides that "classified information originating in one U.S. department or agency shall not be disseminated beyond any recipient agency without the consent of the originating agency" (see Executive Order 12958).

Transmission (5)

To and From Other Government Agencies (a)

DFS serves as the central control point for the receipt and transmission of all FII documents in the NRC. FII documents or matter received by NRC employees must be brought to DFS for proper accountability.

Within the NRC (b)

DFS will promptly transmit any documents containing FII to the appropriate NRC employee having an established need to know. DFS will transmit the documents to the authorized recipient or, in the recipient's absence, to another identified employee with an established need to know who will ensure delivery is made to the intended recipient. (i)

NRC personnel may receive Secret or Confidential documents containing FII at local area meetings or seminars and transport them to their offices, provided they are authorized to hand-carry classified information and comply with the provisions of Part I(C)(3) of this handbook. (ii)

NRC personnel with proper access authorization may transport FII documents or matter within the same NRC installation (see Part I(C)(3) of this handbook). In all instances of delivery of FII to NRC employees, offices, or divisions, recipients shall notify INFOSEC when FII document(s) are received. (iii)

Control of Documents (C) (continued)

Transmission (5) (continued)

Between Installations (c)

Top Secret documents containing FII must be hand-carried by an appropriately cleared and designated NRC courier or by other means approved by the Director, DFS, on a case-by-case basis. Secret or Confidential documents containing FII may be transmitted by appropriately cleared personnel designated by their office director and with a current hand-carry authorization letter from the Director, DFS, or by U.S. registered mail. FII may be transmitted over secure telecommunications systems that have been approved by the Director, DFS.

Abroad (d)

Secret or Confidential documents containing FII may be transmitted to authorized U.S. Government, U.S. Armed Forces, or NRC personnel in foreign countries through the Department of State diplomatic pouch in accordance with Part I(C)(3) of this handbook, or by NRC secure telecommunications systems. Arrangements for transmission of Top Secret documents containing FII will be made through the Director, DFS.

Required Envelopes or Wrappers (e)

When a document or material containing classified FII is sent by U.S. mail or courier outside the agency, it must be enclosed in two opaque envelopes or wrappers. Each inner envelope or wrapper must bear all applicable intelligence markings in addition to the classification marking (see Part I(B)(3) of this handbook). (i)

When FII is hand-delivered by a custodian within the NRC, NRC Form 188A or 188B will be used (see Management Directive (MD) 12.1, "NRC Facility Security Program"). Double envelopes are not required. (ii)

NRC Form 126, "Classified Document Receipt," and NRC Form 253, "NRC Messenger/Courier Receipt," will be used for all FII document or matter transmissions. (iii)

Cover Sheets (f)

When FII is transmitted from one custodian to another inside or outside NRC, one of the following cover sheets will be used: (i)

Control of Documents (C) (continued)

Transmission (5) (continued)

- Standard Form (SF) 703 for Top Secret information (*a*)
- SF 704 for Secret information (*b*)
- SF 705 for Confidential information (*c*)

Custodians will use SF cover sheets stamped with the words "FOREIGN INTELLIGENCE INFORMATION" for easy recognition of FII within the NRC. (ii)

Accountability (6)

Centralized Control (a)

DFS maintains centralized control of all classified documents containing FII received by NRC. In addition, each office or division subsequently receiving FII documents must maintain accountability for them.

Access Sheets (b)

Access sheets must be used for FII documents. DFS will attach an access sheet to each FII document or group of documents filed or distributed within the NRC. All personnel having access to the document(s) will sign and date the access sheet. (i)

Each NRC employee having custodial responsibility for FII documents will ensure that access sheets are attached and used on all FII documents in his or her possession. (ii)

Custodians shall retain access sheets attached to Confidential or Secret FII documents for a period of 2 years, even though the document may have been destroyed. The access sheet will remain attached to any Confidential or Secret FII document. The DFS custodian will retain access sheets attached to Top Secret FII documents for 5 years, even if the document has been destroyed. The access sheet will remain attached to any filed Top Secret document. (iii)

Any deviations from the procedures pertaining to the use of access sheets must be approved by the Director, DFS. (iv)

Control of Documents (C) (continued)

Classified Meetings or Presentations (7)

Classified meetings or presentations that contain FII impose additional requirements on the individual responsible for organizing or arranging these meetings (see MD 12.3, "NRC Personnel Security Program," for further information). (a)

The sponsor of a meeting shall contact DFS before the meeting to ensure that each NRC employee attending has the proper access authorization and has been identified as having a need to know. DFS will provide guidance to the sponsor regarding necessary security precautions when arranging a meeting or presentation. (b)

The sponsor will ensure that all classified notes taken during such meetings are reviewed for proper classification and appropriate intelligence markings. DFS and other authorized classifiers are available to assist the sponsor if necessary. (c)

Storage (8)

Type of Security Containers (a)

Documents or matter containing classified FII must be stored only in approved containers (see MD 12.1).

Access to Containers (b)

Access to containers storing FII must be limited to those NRC personnel who are identified as having a need to know and having the proper access authorization and access to FII.

Changes to Security Container Combinations (c)

DFS personnel only may make changes to combinations of security containers storing FII at the NRC headquarters. Contract guards are not authorized to change combinations of containers storing FII. (i)

Regional offices are responsible for the proper storage of FII security container combinations. Regional offices will ensure that only personnel identified as having a need to know for FII and having the proper access authorization may change combinations. (ii)

Use Standard Form 700 to record and file security container information. When an SF 700 is completed for a containers storing FII, Parts 2 and 2A of the form will be forwarded to INFOSEC for classified storage. Proper classification and marking of the form is required. (iii)

Control of Documents (C) (continued)

Destruction (9)

Only persons who have custody of documents or material containing classified FII and who are authorized access may destroy the material. If a means of destruction is not available, the documents or matter may be brought to DFS for destruction. FII documents will not be placed in data discard containers in NRC buildings because contract guards who collect this material for destruction are not authorized access to FII. All shredders used for the destruction of FII must be approved by the Director, DFS.

Unauthorized Disclosure of Classified FII (D)

Notify immediately the Director, DFS, in the event of loss or possible compromise of classified FII. Upon notification, DFS will conduct an inquiry, including a preliminary assessment of the damage to NRC's mission or to national security. DFS will refer the preliminary assessment, as warranted, to the Executive Director for Operations, the Office of Investigations, the Office of the Inspector General, or the Chairman. A report will be sent to appropriate members of the intelligence community if the inquiry indicates that an unauthorized disclosure has taken place.

Classification, Declassification, or Downgrading (E)

Contact the Director, DFS, regarding questions or actions involving classification, declassification, or downgrading of FII.

Part III

Special Handling of Classified Information

Control of Top Secret Documents (A)

Access to Top Secret information may be granted only to those who possess the appropriate access authorization and the need to know and who have been granted specific written authorization by their office director or regional administrator.

Top Secret Control Officers (1)

Central Top Secret Control Officer (a)

The Director, Division of Facilities and Security (DFS), Office of Administration, has assigned central control functions for Top Secret information to the Information Security Branch (INFOSEC) and has appointed a Central Top Secret Control Officer (CTSCO) and alternates from INFOSEC to ensure efficient operation of the central control functions for Top Secret information. These functions include the assignment of control numbers and, when applicable, series designators for all Top Secret documents, as well as accountability and inventory responsibilities. (i)

All Top Secret documents originated or received by NRC or its contractors must be processed through the CTSCO. (ii)

- Top Secret documents originated by NRC or its contractors working in the headquarters area must be delivered immediately to the CTSCO. (Authority to originally classify NRC documents or NRC contractor documents at the Top Secret level is limited to the Commissioners, the Executive Director for Operations, and the Deputy Executive Director for Management Services.) (*a*)
- Top Secret documents received from other agencies by NRC or NRC contractor personnel in the headquarters area must be delivered immediately to the CTSCO. (*b*)

Control of Top Secret Documents (A) (continued)

Top Secret Control Officers (1) (continued)

- Top Secret documents originated by NRC regional offices or NRC contractor personnel outside the headquarters area, or received from other agencies, must be immediately reported by telephone to the CTSCO. The regional office or contractor must handle and control the document in accordance with instructions received from the CTSCO. (*c*)

Top Secret Control Officers (b)

The Director, DFS, designates Top Secret control officers for each office or division that possesses Top Secret documents. (i)

Top Secret control officers shall receive, transmit, and maintain accountability records for Top Secret documents handled by their offices or divisions. (ii)

NRC and NRC contractor offices with Top Secret storage facilities, approved by DFS, may elect to have Top Secret documents delivered directly from the CTSCO to the authorized addressee or through a designated control point (e.g., office of a Top Secret control officer). (iii)

In either case, the Top Secret document must be charged to the individual who assumes custody of the document. (iv)

Accountability Control Files (2)

Accountability records maintained by the CTSCO must identify all Top Secret documents possessed by NRC and NRC contractors. This accountability must include the current location or storage of each document and the name of the custodian for each document. Accountability files must be maintained as follows:

Document Register (a)

The document register is a permanent record maintained and updated, as appropriate, by the CTSCO. Upon receipt or origination of a Top Secret document by NRC or NRC contractors, the following information is recorded on the document register:

- NRC-assigned document control number and all other documentation information (e.g., series, copy number, and total number of pages) (i)

Control of Top Secret Documents (A) (continued)

Accountability Control Files (2) (continued)

- Document title or subject (ii)
- Date of document (iii)
- Date of receipt or origination (iv)
- Originating NRC office, NRC contractor, or outside agency (v)
- Classification and category (National Security Information, Restricted Data, Formerly Restricted Data) and control caveats (vi)

Receipts File (b)

The receipts file contains records of NRC Form 253, "NRC Messenger/Courier Receipt," and NRC Form 126, "Classified Document Receipt," that have been signed by recipients to whom copies of Top Secret documents were transmitted. This file also identifies the current authorized custodian (e.g., Top Secret control officer or, if none, the recipient) of each Top Secret document in circulation or in storage outside of DFS.

Document History File (c)

The document history file contains a copy of NRC Form 253 and NRC Form 126 for Top Secret documents forwarded to another agency and copies of NRC Form 124, "Top Secret Access Log," for Top Secret documents that have been downgraded, declassified, or destroyed. This file also contains copies of all other pertinent information that the CTSCO deems necessary to ensure a complete history of actions associated with each Top Secret document (e.g., downgrading or declassification notices or destruction authority).

Assignment of a Control Number to Documents From Other Agencies (3)

The CTSCO assigns a unique NRC control number to each Top Secret document received by NRC or NRC contractors from another agency. The control number will be a four-digit number preceded by the symbol "OA-NRC" (e.g., OA-NRC-0000). This number must be placed on the upper right side of the face of the document, the cover, the title page, or the first page of text above any existing documentation.

Control of Top Secret Documents (A) (continued)

Physical Inventory (4)

Top Secret documents under the control of the CTSCO, as well as Top Secret documents charged out to authorized recipients, must be inventoried annually under the direction of the CTSCO. This inventory must be completed by July 31 of each year. (a)

The CTSCO will initiate the inventory and prepare an inventory record listing from the accountability control files. The following identification will be provided for each Top Secret document: the control number, abbreviated title or subject, copy number and series, document date, date of transfer to the authorized holder, and name of the person to whom the document is currently charged. (b)

The CTSCO will forward the inventory record listing of those Top Secret documents sent to authorized recipients to each person charged with the custody of the documents involved. The custodian shall physically account for each document identified and verify the accuracy of the information listed. He or she will report immediately by telephone to the CTSCO any discrepancies and record these discrepancies in the space provided for that purpose on the listing. After completing the inventory of the Top Secret documents charged to him or her, the custodian shall sign and date the inventory record listing and return it to the CTSCO on or before the specified completion date. (c)

Only the following forms, which are available upon request from DFS, are authorized for use in recording, transferring, or receiving Top Secret documents: (d)

- NRC Form 124, "Top Secret Access Log," must be personally signed by each person who has access to the document. (i)
- NRC Form 253, "NRC Messenger/Courier Receipt," and NRC Form 126, "Classified Document Receipt," must be used when transmitting a Top Secret document to authorized custodians. (ii)
- Standard Form 703, "Top Secret Cover Sheet," must be placed on the face of each copy of a Top Secret document upon preparation or upon receipt from outside sources if no form is attached. The cover sheet must remain on each copy at all times whether the copy is held by NRC, NRC contractors or subcontractors, or transmitted to other destinations, until the copy is destroyed. Upon destruction of the documents, the cover sheet may be removed and, depending on its condition, reused. (iii)

Control of Top Secret Documents (A) (continued)

Reproduction of Top Secret Documents (5)

Only the CTSCO may reproduce Top Secret documents. (a)

To reproduce the original set of a Top Secret document (Series A), the originator of the Top Secret document, after consultation with the CTSCO, shall deliver the document to the CTSCO, who will reproduce the number of copies required for distribution. (b)

Reproduction of subsequent sets of a Top Secret document (e.g., Series B, C, D, etc.) after the original set will be authorized only in an extreme emergency. When such emergencies exist, a written request describing the circumstances that justify reproduction must be submitted to the Director, DFS. (c)

If the request is approved, the CTSCO will reproduce the document. The CTSCO shall assign the copy(ies) the next series designator (e.g., B, C, D, etc.) and record all pertinent information required in Sections (A)(3) and (4) of this part. The requester shall ensure that the following statement is placed on the upper right side of the copy(ies) underneath the existing documentation and that it is accurately completed: (d)

"Series _____Copy_____ of_____copies."

The written request for reproduction and the authorization for reproduction signed by the Director, DFS, must be affixed to the document used to prepare the additional copies. (e)

If the request is disapproved, the Director, DFS, shall so advise the requester in writing. (f)

Reproduction of Top Secret Documents From Other Agencies (6)

Top Secret documents or portions of documents containing Top Secret information originated by another U.S. Government agency or one of its contractors must not be reproduced unless written approval is obtained from the agency that originated the document. The individual wishing to reproduce this information shall obtain written approval from the agency involved. Upon receipt of this approval, the individual shall request the CTSCO to reproduce the information.

Control of Top Secret Documents (A) (continued)

Transmission of Top Secret Documents (7)

Top Secret documents may only be transmitted by NRC and NRC contractor employees authorized this authority by the Director, DFS (e.g., NRC courier, Top Secret control officer, or an alternate). The Defense Courier Service or other means must be approved by the Director, DFS, on a case-by-case basis. Under no circumstances may Top Secret documents be transmitted through the U.S. Mail or other NRC or NRC contractor internal mail service. (a)

Top Secret information must be transmitted, to the maximum extent possible, by discussions between authorized persons in areas prescribed by the Director, DFS, or by secure communications approved by the Director, DFS. Otherwise, Top Secret information must be hand-delivered by authorized persons within the same building, or by NRC authorized couriers or the Defense Courier Service when Top Secret information must be delivered to other buildings, facilities, or Government agencies. Persons hand-carrying Top Secret documents shall keep the documents continuously in their possession until the information is stored in an approved facility or is turned over to a designated recipient. (b)

Before transmission or transfer of any Top Secret document, the CTSCO shall be consulted. Approval for NRC contractor employees to hand-carry classified documents during travel via commercial airlines must be obtained from the Director, DFS. Additionally, the Federal Aviation Administration has issued regulations for screening travelers and matter transported by air. (c)

Receipts (8)

NRC Forms 253 and 126 must be used to transfer all NRC-originated or NRC-possessed Top Secret documents to authorized individuals in NRC or NRC contractor organizations or to other agencies or their contractors.

Destruction of Top Secret Documents (9)

The CTSCO or alternates are authorized to destroy Top Secret documents. Whenever, Top Secret documents are destroyed, a second NRC employee or NRC contractor employee shall witness the destruction and certify it by signing the destruction record along with the CTSCO or alternates. (a)

Control of Top Secret Documents (A) (continued)

Destruction of Top Secret Documents (9) (continued)

Top Secret documents must be destroyed by shredding, and Top Secret waste (e.g., paper, or computer disks) must be destroyed in accordance with instructions received from CTSCO. (b)

Naval Nuclear Propulsion Information (B)

U.S. naval nuclear propulsion information, either classified or unclassified, must be made available on a need-to-know basis only to NRC employees and NRC contractor employees who are United States citizens. (1)

When an NRC office determines that an NRC contractor requires classified or unclassified naval nuclear propulsion information, the office will forward written justification for access to the Office of Naval Reactors, Department of Energy (DOE), with an information copy to DFS. DFS also is available to provide assistance. (2)

Public release of classified or unclassified naval nuclear propulsion information, or foreign release thereof, is not permitted. In accordance with regulation (10 CFR 9.25(d)), any request from a source outside the NRC for nuclear propulsion documents or information must be forwarded through the Office of the Chief Information Officer (OCIO) to the Office of Naval Reactors, DOE, for disposition. (3)

Classified naval nuclear propulsion information and documents must be protected and handled in accordance with existing security directives. (4)

The Office of Naval Reactors, DOE, in providing either classified or unclassified naval nuclear propulsion documents to the NRC, marks documents with the statement given below. Any exact reproductions of documents that bear this marking or preparation of other documents containing naval nuclear propulsion information derived from the original documents must contain this marking. (5)

> This document may not be further distributed by any holder without the prior approval of the Office of Naval Reactors, United States Department of Energy. Distribution to United States nationals representing foreign interests, foreign nationals, foreign governments, foreign companies and foreign subsidiaries or foreign divisions of United States companies is specifically prohibited.

National Security Council Information (NSCI) (C)

Responsibilities (1)

Access to classified NSCI must be limited to the absolute minimum number of NRC persons holding a "Q" clearance who have a need to know and who require such access to perform their official duties. All classified NSCI documents in the possession of NRC must be protected. National Security Decision Directive 19 (NSDD-19), "Protection of Classified National Security Council and Intelligence Information," provides the basis for protection. (a)

The Chairman and the EDO may authorize access to classified NSCI for NRC Commission and staff personnel with a "Q" clearance, respectively. (b)

The Commissioners, office directors, and regional administrators may authorize "Q"-cleared members of their own offices access to NSCI. (c)

Any difference of opinion at the Commission level regarding access authorization, period of access, and so forth, must be resolved by the Chairman or, if necessary, by a Commission vote. The EDO will resolve any such differences at the staff level. (d)

Access Lists (2)

Access lists reflecting authorizations must be prepared by the authorizing authority and updated as necessary. The access lists also must specifically designate those individuals who are responsible for initial receipt of NSCI in respective offices. (See Part II (C)(6)(b) of this handbook for more information on access sheets.) (a)

The Offices of the Chairman, Commissioners, and EDO, and other Commission-level offices will each provide a copy of their access list and any changes to the list to the Office of the Secretary (SECY). (b)

Staff-level offices will each provide a copy of their access list and any changes to the Administrative and Correspondence Branch, Office of the EDO. SECY and the Administrative and Correspondence Branch will provide a copy of these access lists to the Director, DFS. (c)

Requirements (3)

Receipt and Handling (a)

All classified NSCI transmitted to NRC by the National Security Council (NSC) will be addressed to the Chairman and, therefore, received by SECY. (i)

National Security Council Information (NSCI) (C) (continued)

Requirements (3) (continued)

SECY will maintain strict control and accountability over all classified documents containing NSCI. (ii)

Upon receipt of NSCI, SECY will—(iii)

- Record the NSC number affixed to the NSC cover sheet. (*a*)
- Determine who at the Commission level requires access to the information and record the names of the offices on the NSC cover sheet. (*b*)
- Forward the NSCI document to the responsible individual designated on the intended recipient's access list. (*c*)
- Ensure that the document and the NSC cover sheet are returned to SECY for storage after completion of the required circulation and review. (*d*)

If the NSCI document is to be distributed at the staff level, the EDO Administrative and Correspondence Branch will duplicate steps (a) through (d) of item (iii) above for appropriate distribution. (iv)

Upon return of the document from the staff, the EDO Administrative and Correspondence Branch also will forward the NSC cover sheet generated for staff distribution to SECY for storage with the document. (v)

In the event an office receives classified NSCI by means other than those described above, that office will immediately notify SECY. SECY will obtain the NSCI document from the office and follow the procedures under item (iii) above to ensure proper control and accountability. SECY also will notify DFS staff, who will conduct an inquiry into the matter and take the necessary action to prevent recurrence. (vi)

All authorized individuals having access to a classified document containing NSCI shall sign the NSC cover sheet accompanying the document. If an authorized individual is only responsible for distribution of the document (e.g., SECY, EDO Administrative and Correspondence Branch, a designated individual of an office), this individual shall indicate this fact by placing the symbol "DO" (for "distribution only") after his or her signature on the cover sheet. (vii)

National Security Council Information (NSCI) (C) (continued)

Requirements (3) (continued)

Reproduction (b)

Documents containing NSCI will be reproduced only when it is determined that the document must be circulated quickly to facilitate a timely NRC response. The determination that a classified document containing NSCI needs to be reproduced will be made by SECY. Only SECY may reproduce classified NSCI documents. (i)

After making the required copies, SECY will complete and affix an NSC cover sheet to each copy of the document. Above the NSC number on the cover sheet, SECY will place "NRC Copy_____" and assign a sequential alphabetical designator (i.e., A, B, C, etc.) to each copy of the document. (ii)

Documents Generated by NRC (c)

The NRC does not routinely generate documents that contain classified NSCI. However, in the event an office does generate a document that contains classified NSCI, the document and any drafts and work sheets must be protected. Additionally, the office generating the NSCI document must contact DFS to obtain guidance for accountability of the document.

Loss or Possible Compromise of Documents (d)

DFS must be notified immediately in the event of loss or possible compromise of a classified NSCI document. Staff offices shall submit a written report on any such matter to the Chairman through the EDO. Commission offices shall submit a written report on any such matter to the Chairman. DFS will report a loss or a possible compromise to NSC and conduct an inquiry into the matter. A written report on the matter, including corrective measures taken, where appropriate, shall be submitted by the EDO to the Chairman.

Classification, Declassification, or Downgrading (e)

Any classification, declassification, or downgrading questions on NSCI must be referred to DFS for advice and assistance.

National Security Council Information (NSCI) (C) (continued)

Requirements (3) (continued)

Requests for Information Under the Freedom of Information Act (f)

SECY, in consultation with the Office of the General Counsel, will determine what NSCI records, if any, are subject to the Freedom of Information Act (FOIA). The OCIO must be notified when NSCI records are the subject of FOIA request. OCIO will be responsible for referring the records to the NSC.

Transfer of Classified Information to Foreign Governments and International Organizations (D)

Authorities (1)

Classified Nonmilitary Information (a)

The Presidential Directive of September 23, 1958, "Basic Policy Governing the Release of Classified Defense Information to Foreign Governments," specifies policy governing the transfer of classified nonmilitary information to foreign governments and access to classified nonmilitary information by individual representatives of foreign governments.

Classified Military Information (b)

Basic policy governing the release and disclosure of classified military information is specified in "National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations," and supplemented by National Security Decision Memorandum (NSDM)-119, "Disclosure of Classified Military Information to Foreign Governments and International Organizations.

Restricted Data and Formerly Restricted Data (c)

The provisions of Section (D) of this part do not apply to the transmission of Restricted Data or Formerly Restricted Data to foreign governments or international organizations. Restricted Data and Formerly Restricted Data are furnished to and received from foreign governments and international organizations only in accordance with Agreements for Cooperation negotiated in accordance with the provisions of Sections 123 and 144 of the Atomic Energy Act of 1954, as amended (AEA).

Transfer of Classified Information to Foreign Governments and International Organizations (D) (continued)

Authorities (1) (continued)

Prohibitions on Disclosure (d)

The disclosure of classified information to foreign governments or international organizations is not permitted when such disclosure is prohibited by Presidential orders or directives, Federal legislation, including the AEA, and the Energy Reorganization Act of 1974 (ERA), as amended, or by any international agreement to which the United States is a party, or by United States policy.

Criteria (2)

Criteria for Release of Classified Information to Foreign Governments (a)

The following criteria must be satisfied before the release of classified nonmilitary information to foreign governments.

- A determination that the furnishing of classified information will result in a net advantage to the national security interests of the United States must be made. In making this determination, disclosure is—(i)
  - Consistent with the foreign policy of the United States toward the recipient government (*a*)
  - Consistent with the policies of the U.S. Government with regard to the AEA, the AEA, or with regard to information for which special procedures for release have been or may hereafter be established by competent authority having statutory jurisdiction over the subject matter (*b*)
  - Consistent with the national security interests of the United States (*c*)
  - Limited to information necessary to the purpose for which disclosures made (*d*)

Transfer of Classified Information to Foreign Governments and International Organizations (D) (continued)

Criteria (2) (continued)

- The recipient government must have agreed, either generally or in the particular case, to—(ii)
  - Not release the information to a third party without the approval of the releasing party (*a*)
  - Afford the information substantially the same degree of protection afforded it by the releasing party (*b*)
  - Not use the information for other than the purpose for which it was given (*c*)
  - Respect rights such as patents, copyrights, or trade secrets, in the event that the releasing party indicates private rights are involved in the information. (*d*)

Criteria for Release of Classified Information to International Organizations (b)

The release of classified information to international organizations, with the exception of the International Atomic Energy Agency (IAEA) noted in the next paragraph, must be on the basis of criteria identified in Section (D)(2)(a) of this part. However, these criteria will be addressed on a case-by-case basis for each transmittal, taking into account the particular reason for providing classified information to that organization. (i)

The Commission has determined that the release of classified information to IAEA, as agreed upon by the U. S./IAEA Safeguards Agreement, will result in a net advantage to the national security interest of the United States. Furthermore, Article 5 of the U.S./IAEA Safeguards Agreement satisfies the criteria of Section (D)(2)(a) of this part. The criterion of Section (D)(2)(a) of this part has been waived by the Commission. (ii)

Responsibilities (3)

The Director, Office of International Programs (OIP), will determine that the furnishing of classified information will result in a net advantage to the national security interests of the United States. The

Transfer of Classified Information to Foreign Governments and International Organizations (D) (continued)

Responsibilities (3) (continued)

determination must be made with the concurrence of the Office of the General Counsel (OGC), DFS, and the responsible program office. OIP will consult with the Department of State and other agencies and departments, as appropriate, in making this determination. OIP also will initiate and coordinate the procedural process to implement the proposed classified information transfers.

Classified Information Exchange Agreements With Foreign Governments (a)

Before the development of an exchange agreement, DFS will determine whether an applicable government-to-government agreement exists between the United States and the foreign country involved. (i)

If no agreement exists, DFS, with the assistance of OIP and OGC, will develop a separate classified information exchange agreement for each foreign government agency involved before initial transfer of classified information or before initial written or oral access. This information exchange agreement must specify the requirements necessary to ensure the security of the transferred classified information. The agreement will be compatible with the terms and conditions of existing government-to-government agreements applicable to the transfer of classified information. (ii)

The EDO shall execute the exchange agreement upon a finding that the recipient government will provide adequate protection of the classified information to be furnished. The Commission will be informed by OIP before the execution of any international agreement. (iii)

The Commission will approve any waiver of the required understandings identified in Section (D)(2)(a) of this part concerning the criteria specified. (iv)

Agreements with foreign governments will not commit the NRC to disclose any particular or specific classified information. (v)

Transfer of Classified Information to Foreign Governments and International Organizations (D) (continued)

Responsibilities (3) (continued)

Classified Information Exchange Agreements With International Organizations (b)

The release of classified information to international organizations, with the exception of the IAEA, will be addressed on a case-by-case basis for each transmittal, considering the particular reason for providing classified information. Therefore, before permitting representatives of international organizations (with the exception of the IAEA) access to classified information, DFS must be consulted. (i)

DFS will coordinate the matter with OIP, OGC, and others, as appropriate, and approve or disapprove the access. If the access is approved, DFS will provide appropriate guidance to effect access or transmittal. (ii)

Internal Procedures (4)

Transfer of Classified Information to Foreign Governments (a)

Security Assurance and Security Checks (i)

A security assurance must be required and a security check made regarding the original recipients of classified information. (*a*)

OIP will obtain the security assurance and the background and biographical data on NRC Form 70, "Request for Name Check," and submit this information to DFS with request that the appropriate security check be conducted. (*b*)

The EDO is authorized to waive the requirement for a security assurance and/or a security check for high-ranking foreign government civil or military representatives when necessary. (*c*)

Results of Security Checks (ii)

The existence of security assurances and the results of any security checks, when applicable, must be made a matter of record in DFS. DFS shall make available any derogatory information derived from security checks on a confidential basis to only the Director, OIP, and the EDO.

Transfer of Classified Information to Foreign Governments and International Organizations (D) (continued)

Internal Procedures (4) (continued)

Review of Documents To Be Transferred (iii)

Classified documents to be transmitted to foreign governments must be forwarded to DFS for review and transmission. (*a*)

The review must ensure that—(*b*)

- Each original recipient possesses a prescribed security assurance; a security check of each original recipient has been conducted; and the results of the security check are favorable or a waiver has been obtained. (*i*)
- The information transmitted is within the scope of the government-to-government agreement negotiated with the country concerned and the classified information exchange agreement negotiated with the foreign government agency to which the documents are being furnished. (*ii*)
- Concurrence in the legal aspects of the transfer has been obtained from OGC. (*iii*)

If the transfer involves classified documents or other classified information originated, produced, or received from another department or agency, DFS will obtain approval from this department or agency. (*c*)

Accountability (iv)

A record of accountability of the information being processed for release must be maintained by DFS and by each NRC office or division proposing the release of classified nonmilitary information to foreign governments or concurring in the release. (*a*)

The record must include—(*b*)

- Identification of the exact information released or being processed for release (for documents, the date, title, name of originator, and classification) (*i*)
- Names and signatures of approving officials (*ii*)

Transfer of Classified Information to Foreign Governments and International Organizations (D) (continued)

Internal Procedures (4) (continued)

- Form in which information is released or will be released (e.g., oral or documentary) (*iii*)
- Date of release or contemplated release (*iv*)
- Identity of foreign government organization to which and original individual recipient to whom release is made or is contemplated (*v*)
- Security assurance and security check, when applicable, for each individual recipient (*vi*)
- Waivers exercised or requested, when applicable (*vii*)
- Statement that the information is based on data originated outside NRC, wherever applicable, and the identity of the originating organization (*viii*)
- Name of individual in other United States Government agency who has authorized release, if applicable (*ix*)

The office or division contemplating or making oral disclosures must furnish memoranda before and after these disclosures to the Directors of DFS and OIP, and to OGC. (*c*)

Preparation and Method of Transmission (v)

The preparation (including classification) and method of transmission of documents are specified in Part I(C)(7) of this handbook. Normally, documents intended for a foreign government will be forwarded to that country's embassy in the United States. Transmission of classified mail to foreign countries requires prior approval of the Director, DFS.

Transfer of Classified Information to International Organizations (Except IAEA) (b)

The transfer of classified information to international organizations, except IAEA (see item (c) below), must be handled in accordance with guidance from DFS.

Transfer of Classified Information to Foreign Governments and International Organizations (D) (continued)

Internal Procedures (4) (continued)

Transfer of Classified Information to IAEA (c)

Written Disclosure Authorization (i)

A written disclosure authorization from DFS is required before IAEA representatives may have access to National Security Information. This authorization states that the individual is an authorized IAEA representative and is authorized to make visits or inspections in accordance with the U.S./IAEA Safeguards Agreement. (*a*)

The authorization includes—(*b*)

- The identity of the authorized IAEA representative (*i*)
- Specific authority to disclose National Security Information to that individual relating to the visit or inspection (*ii*)
- The level of classified information authorized (*iii*)
- A description of the IAEA representative's identification documents (*iv*)
- The purpose of the visit or inspection (*v*)
- The duration of the authorization to receive the information (*vi*)

In accordance with authority set forth in the disclosure authorization, classified documents may be furnished to IAEA representatives for retention or may be transmitted to IAEA. (*c*)

Review of Documents To Be Transferred (ii)

Classified documents to be furnished to IAEA representatives by approved means, or transmitted to IAEA representatives, must be reviewed by DFS before release. The review must ensure that the information to be furnished or transmitted is within the scope of the written disclosure authorization. (*a*)

If access or transmission involves classified information originated by another department or agency, DFS will obtain approval from the department or agency before access or transmission. (*b*)

Transfer of Classified Information to Foreign Governments and International Organizations (D) (continued)

Internal Procedures (4) (continued)

Accountability (iii)

See Section (D)(4)(a)(iv) of this part

Preparation and Method of Transmission (iv)

See Section (D)(4)(v) of this part

Report to the National Disclosure Policy Committee (NDPC) (v)

DFS will report to the NDPC those transfers of classified information to foreign governments or international organizations that must be reported under the national disclosure policy. This reporting is required in every instance in which defense information is involved.

Review and Concurrence in Legal Aspects of Transfer (vi)

OGC will review and concur in the legal aspects of NRC transfer of information to foreign governments or international organizations.

Access Lists (5)

Access to Top Secret information and NSCI requires a "Q" clearance, need to know, and the written authorization of the regional administrator or the director of the office sponsoring the activity or in which the individuals seeking access are employed. Each region and office with personnel authorized access to Top Secret information or NSCI will maintain a list of its authorized personnel. (a)

A copy of the access list for each region and office must be provided to DFS. Additionally, a copy of the NSCI access list for each region and office must be distributed in accordance with Part III(C)(2) of this handbook. (b)

Any updates (e.g., additions or changes) of a regional or office access list must be reported immediately to DFS and any other recipient of the list. (c)

Each region and office will review their access lists during January of each year to ensure that all listed personnel need continued authorization and will provide DFS and any other recipient with a revised list on or before January 31 of each year. (d)

Transfer of Classified Information to Foreign Governments and International Organizations (D) (continued)

Sanctions (6)

NRC employees, NRC contractors, and other organizations associated with the NRC program shall be subject to appropriate sanctions if they—(1)

- Knowingly, willfully, or negligently disclose to unauthorized persons information properly classified under EO 12958 or predecessor Executive orders, or the AEA. (a)
- Knowingly and willfully classify or continue the classification of information in violation of EO 12958 or any implementing directive. (b)
- Knowingly and willfully violate any other provision of EO 12958 or any implementing directive, or the AEA relating to the classification and declassification of Restricted Data and Formerly Restricted Data. (c)

Sanctions may include reprimand, suspension without pay, removal, termination of classification authority, loss or denial of access to classified information, or other sanctions in accordance with applicable law and NRC regulations. (2)

Classified Conferences (E)

Conferences and Symposia (1)

At times, NRC employees, NRC contractors, and other organizations affiliated with NRC sponsor or participate in conferences and symposia that are intended to be unclassified but that relate to sensitive programs or installations and may contain classified information. To minimize the risk of inadvertently revealing classified information at these meetings, the procedures below have been established.

- Papers involving sensitive programs or installations are to be submitted to an NRC authorized classifier (see Part I (B)(2) of this handbook) or to DFS for review before unclassified use. (a)

Classified Conferences (E) (continued)

Conferences and Symposia (1) (continued)

- All NRC and NRC contractor personnel who are to deliver briefings that involve sensitive programs or installations shall have the text of such briefings reviewed for classification by an NRC authorized classifier or by DFS before presentation. (b)

Publication or Release of Documents (2)

When there is doubt as to whether a document contains National Security Information, Restricted Data, or Formerly Restricted Data, the author shall refer the information to the appropriate NRC authorized classifier or the Director, DFS, for a classification review.

Review of Documents (3)

An NRC employee, an NRC contractor employee, or another person associated with the NRC program may desire to release, as unclassified, information relating to his or her activity. Contracts for classified work contain clauses that require safeguarding of classified information. To ensure that classified information is properly safeguarded, proposed disclosures, whether in the form of documents, visual materials, speeches, or otherwise, must be reviewed by an authorized classifier to prevent the inadvertent disclosure of classified information, as well as to obtain appropriate review for patent clearance. NRC employees and other personnel associated with the NRC program are under similar obligation to protect classified information against disclosure in conjunction with the release of unclassified information.

Review of Documents Submitted by Uncleared Authors (4)

Documents submitted for review by an uncleared author who, to the best of the reviewer's knowledge, has never had access to classified information, must be forwarded to DFS for review. If, after review, it is determined that the article contains information that should be classified, DFS will advise the author, to the extent possible within the bounds of security, of the reason for the classification and, if possible, take action to have the author delete any classified information contained in the document. In the course of such a review, DFS will refer the document to other NRC offices, to the NRC regions, and to other Government agencies, as appropriate.

Classified Conferences (E) (continued)

Review of Documents Submitted by Formerly Cleared Persons or by Authors With Active Clearances (5)

Documents submitted by persons formerly cleared at the "Q" or "L" level, by persons with active NRC clearances other than those set forth in MD 12.3, "Personnel Security Program," or by persons formerly or currently cleared by other Government agencies must be reviewed by an NRC-authorized classifier or by DFS. The author shall be required to delete any classified information in the document before it is published.

Transporting Classified Material via Commercial Airlines (F)

Approval for NRC contractor employees to hand-carry classified documents during travel via commercial airlines must be obtained from the Director, DFS. Additionally, the Federal Aviation Administration (FAA) has issued regulations for screening travelers and matter transported by air. Accordingly—(1)

- Each NRC employee and NRC contractor employee hand-carrying classified information shall carry his or her travel authorization and his or her NRC identification badge, which has his or her photograph and signature. The employee shall also carry the document authorizing him or her to hand-carry the information. (a)

- All passengers and items transported must be screened before boarding an aircraft. Briefcases or other luggage, including that containing the classified information, may be opened by airport screening personnel for inspection. This inspection must be conducted without opening the envelopes containing classified documents. The screener should be able to inspect the envelopes by flexing, touch, weight, x-ray, and so forth. (b)

- If the screener is not satisfied, the passenger will state that the packages contain classified information. The passenger will present his or her identification card and travel authorization. If the screener is still not satisfied, the passenger should immediately ask to talk to the senior air carrier representative or FAA security representative and explain the situation. If necessary, the traveler will contact his or her own supervisor or DFS. (c)

Transporting Classified Material via Commercial Airlines (F) (continued)

- In instances in which classified documents to be transported are of a size, weight, or shape not suitable for the processing specified above, the following procedures apply: (d)
  - NRC employees or NRC contractor personnel who have been authorized to transport classified documents must notify airline officials at the point of origin and at intermediate transfer points in advance of the trip. (i)
  - Employees carrying packages must report to the airline ticket counter and present documentation and a description of the containers that are exempt from screening. (ii)
  - Employees must have the original correspondence signed by appropriate supervisory personnel authorizing them to carry classified documents. This correspondence must be prepared on letterhead stationery of the NRC or the contractor employing the individuals. (iii)
  - Employees shall have enough authenticated copies of this correspondence to provide a copy to each airline involved. (iv)

The correspondence authorizing an employee to transport classified documents must contain—(2)

- The full name of the employee and the NRC office or the NRC contractor by whom employed (a)
- A description of the type of identification the employee will present (e.g., NRC photo badge) (b)
- A description of the matter being carried (e.g., "Three sealed packages, 9 inches by 8 inches by 24 inches," and the names of the sender and the addressee) (c)
- Identification of the point of departure, destination, and known transfer points (d)
- Date of issue and the expiration date of the correspondence, which is not to exceed 7 days from the date of issue (e)
- Name, title, signature, and telephone number of official authorizing the employee to carry the classified documents (f)

Transporting Classified Material via Commercial Airlines (F) (continued)

- Name and telephone number of the NRC official or the NRC contractor official who can confirm the letter of authorization (g)

Each package or carton to be exempt from screening must be signed on its face by the official signing the correspondence. When an employee is required to transport classified packages on a return trip and the letter from his or her organization does not cover this return trip, a letter of authorization must be prepared on the letterhead stationary of the agency or the contractor being visited. (3)

Exhibit 1

Required Markings for Classified Documents

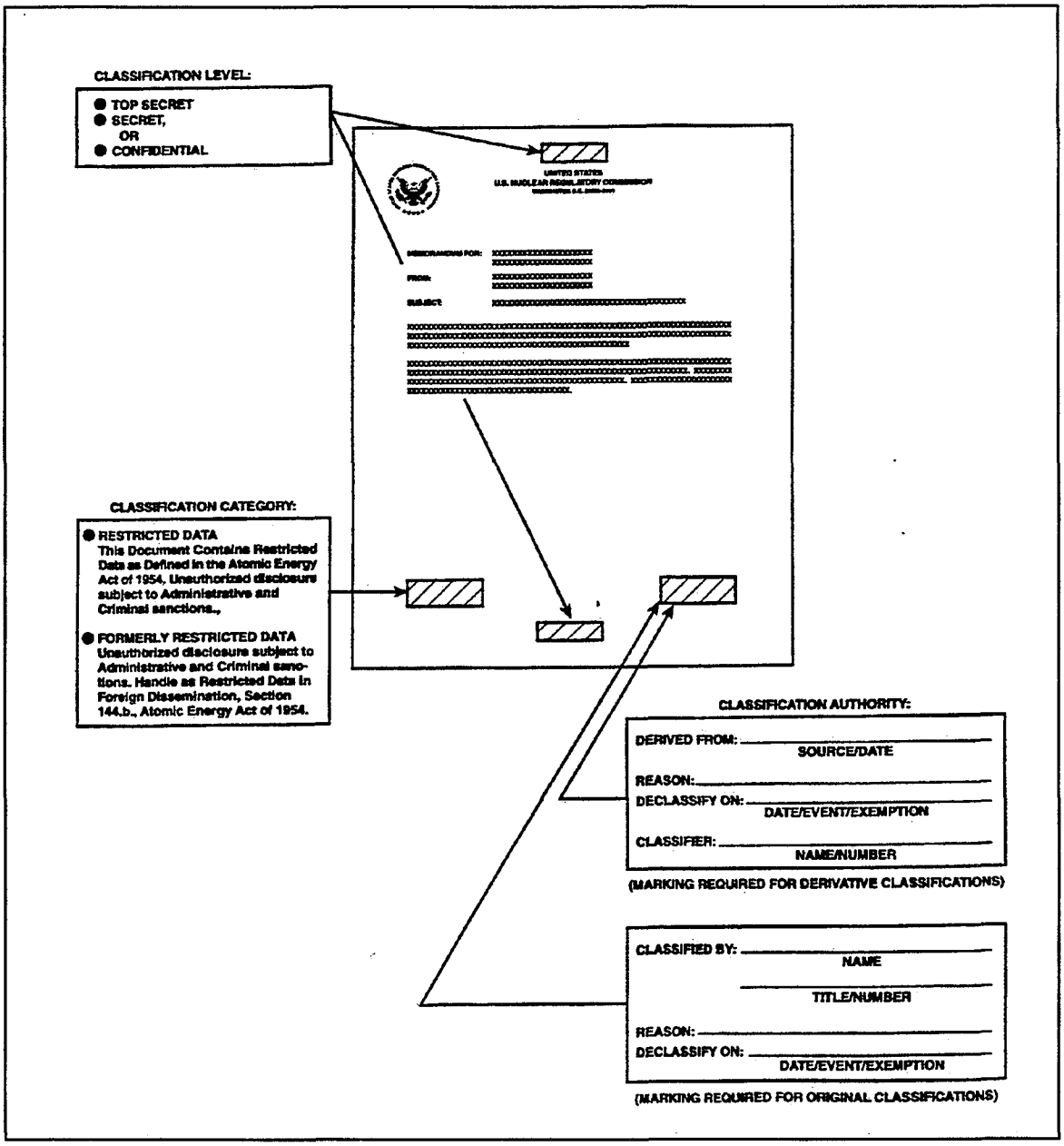


Exhibit 2

Declassification Markings

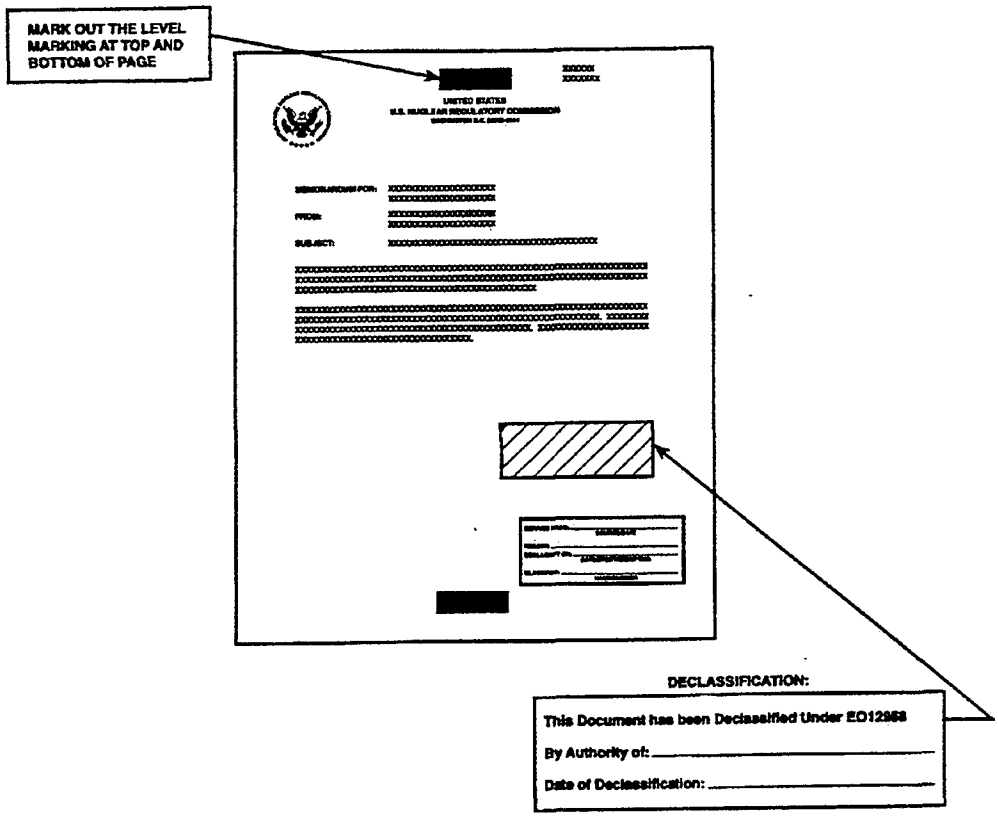


Exhibit 3

Subject or Title Marking and Portion-Marking

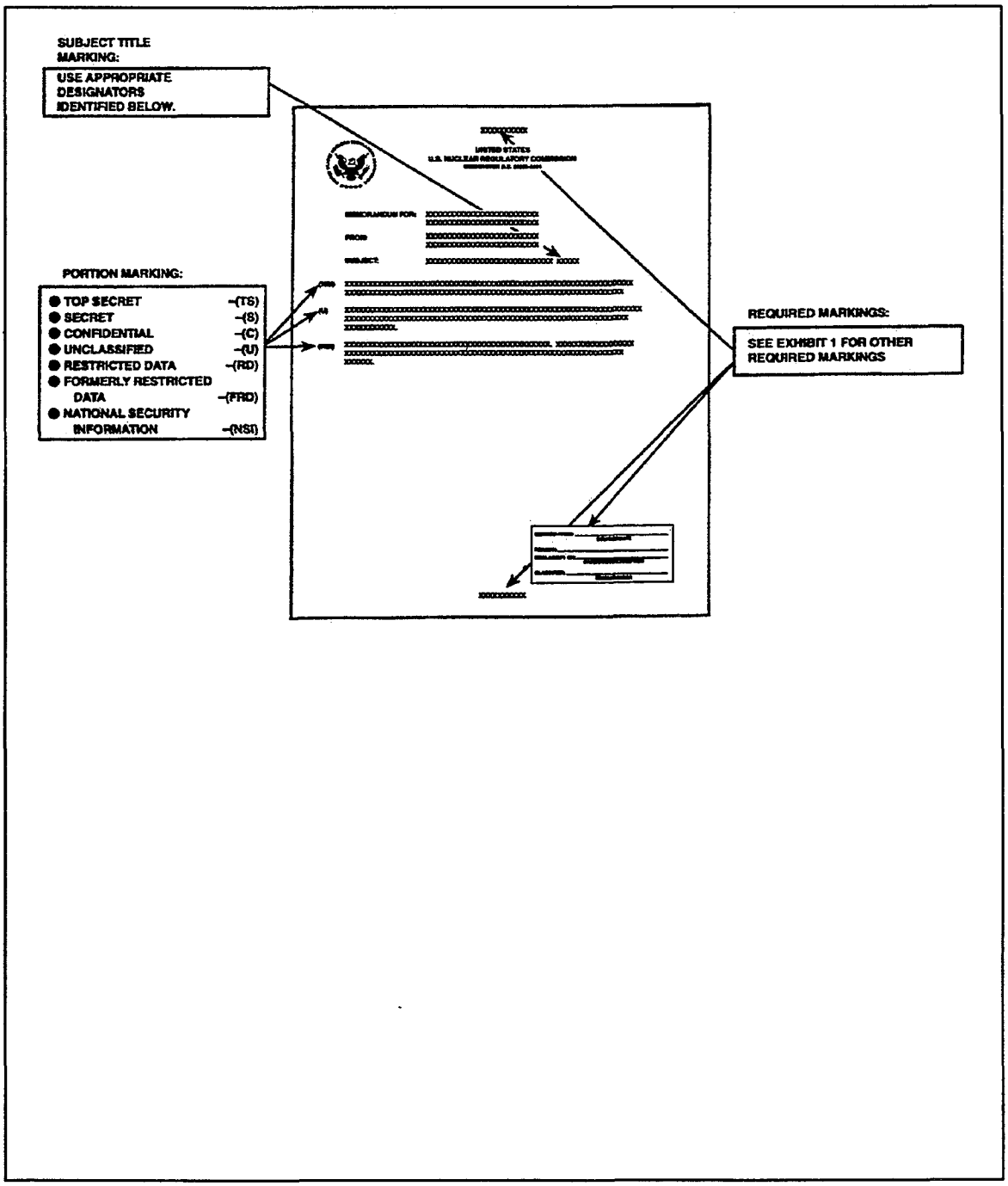


Exhibit 4

Upgrading, Downgrading, and Transclassification Markings

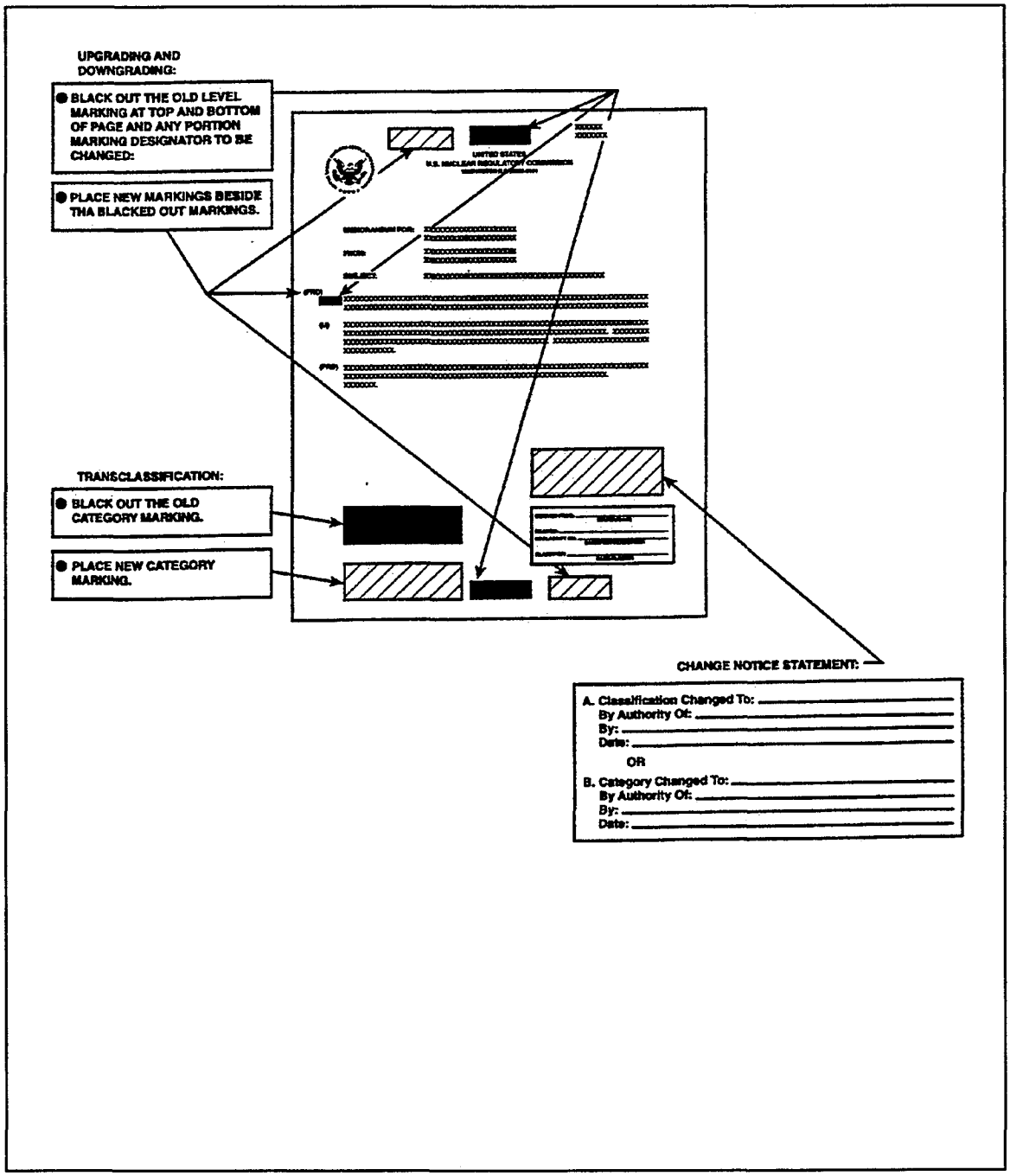


Exhibit 5

Deleting Classified Information From Classified Documents

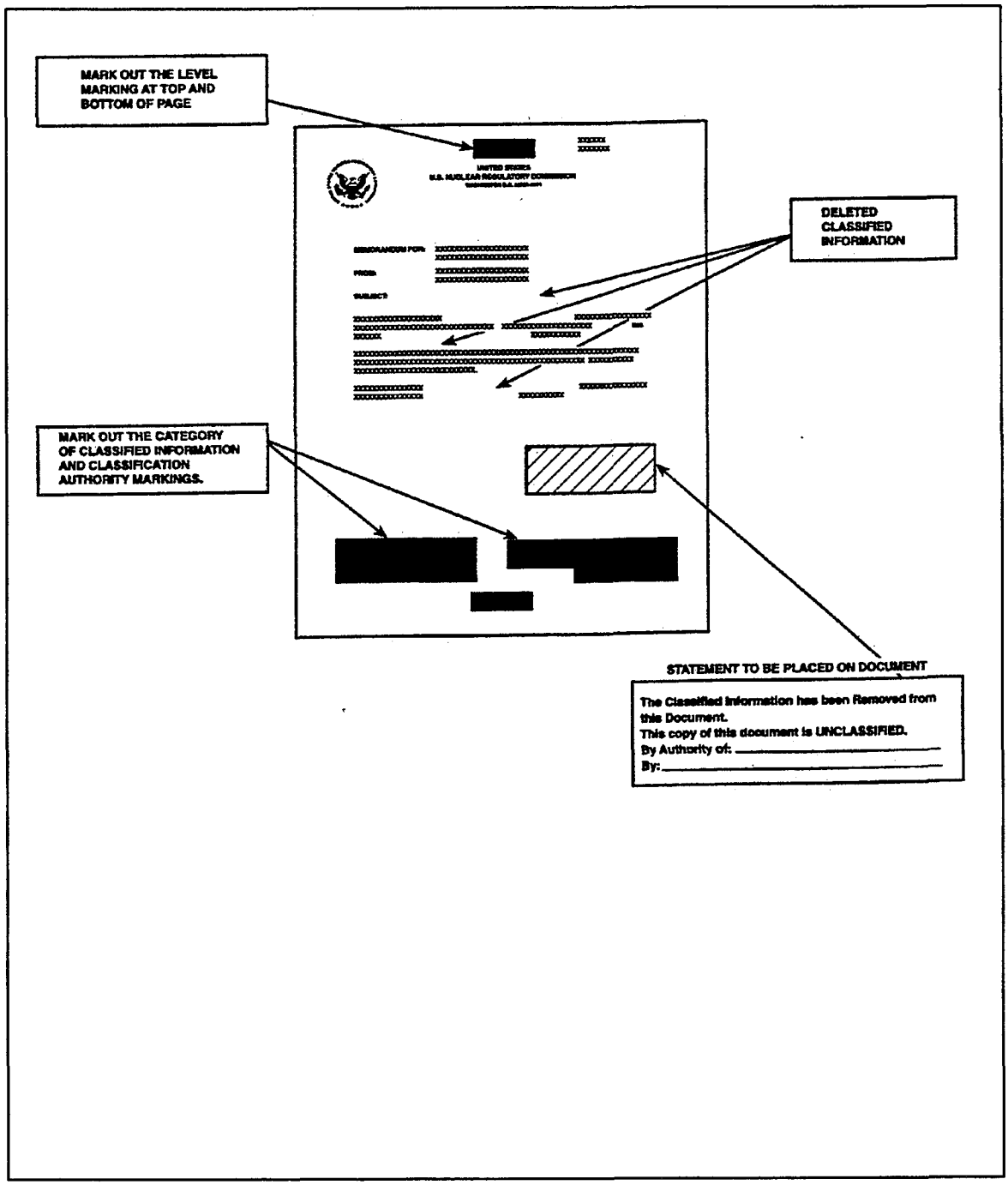


Exhibit 6

Required Markings for Unclassified Transmittal Document

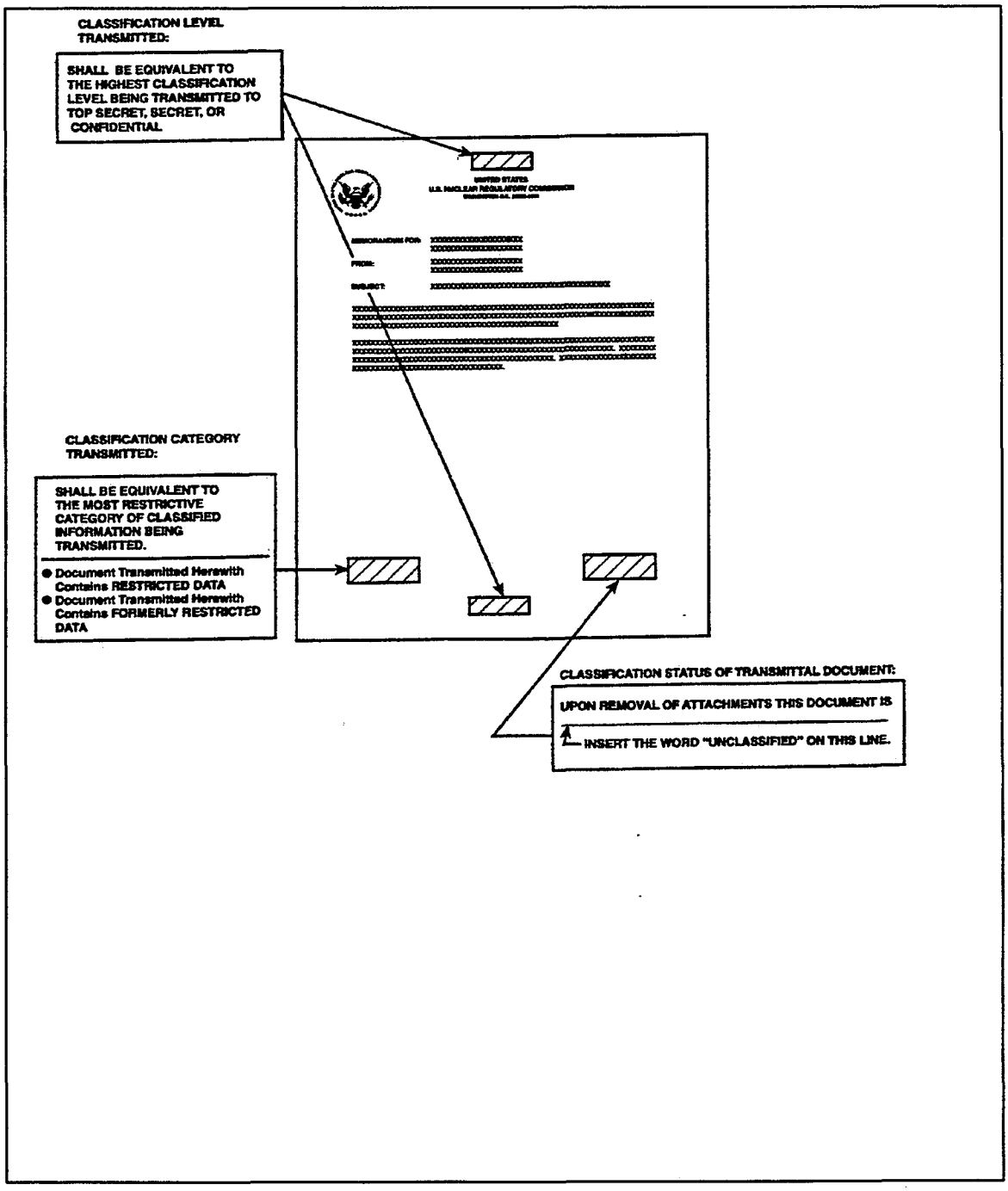


Exhibit 7

Required Markings for Classified Transmittal Document

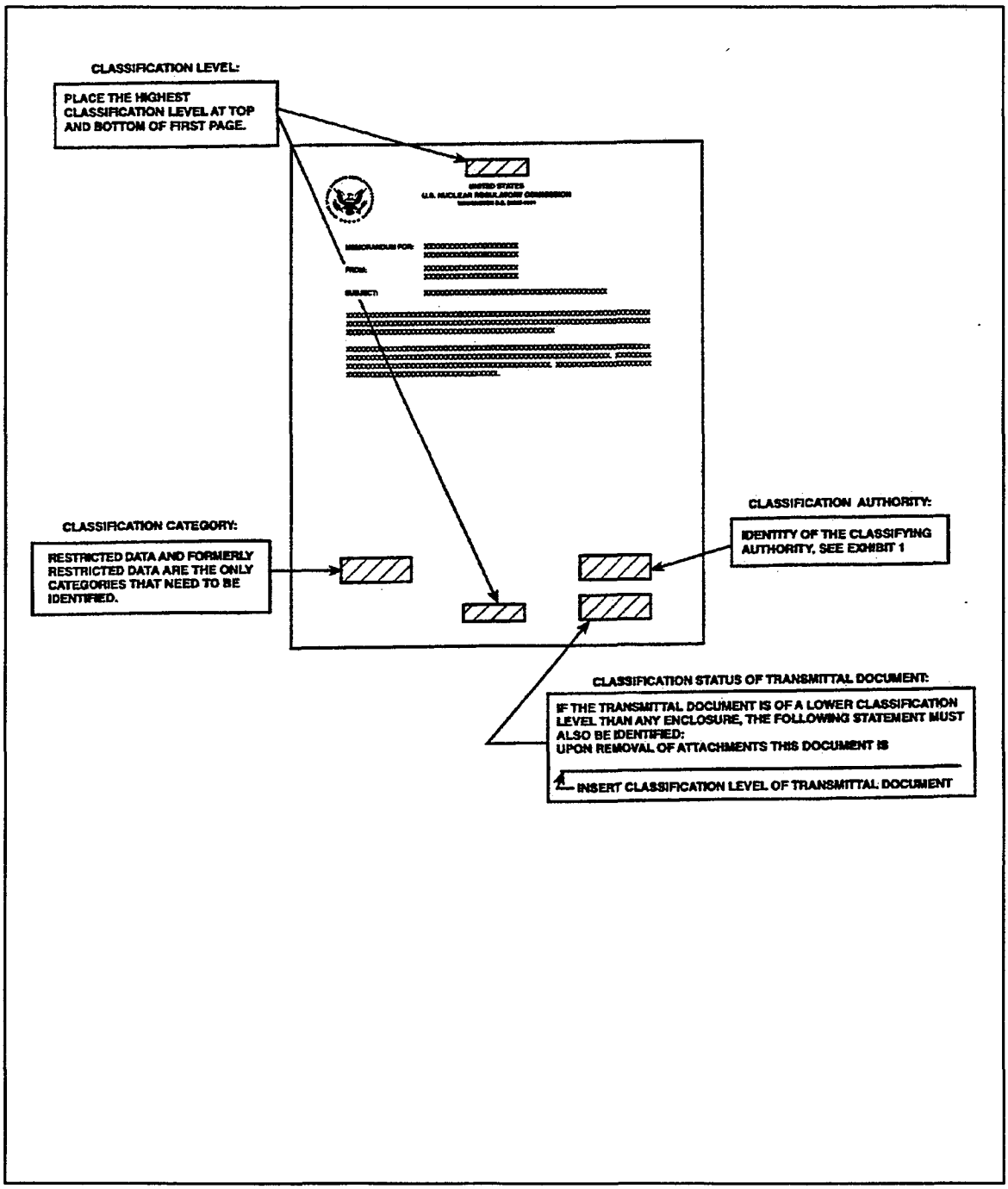
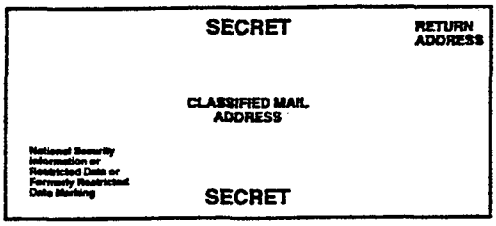


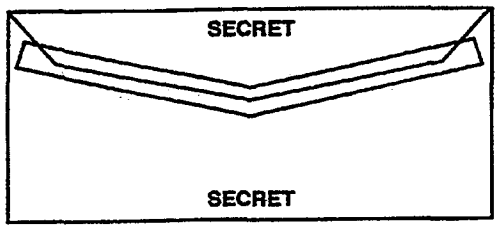
Exhibit 8

Required Markings for Envelopes or Wrappers

INNER ENVELOPE (OPAQUE)
TOP SECRET, SECRET OR CONFIDENTIAL



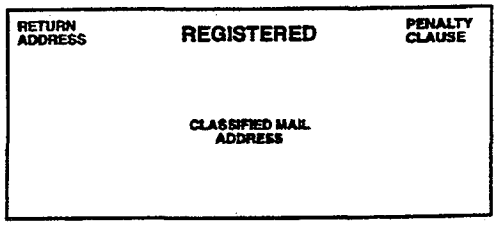
FRONT



BACK

OUTER ENVELOPE (OPAQUE)

SECRET



CONFIDENTIAL

CLASSIFICATION FOR EXHIBIT PURPOSES ONLY

U.S. NUCLEAR REGULATORY COMMISSION

DIRECTIVE TRANSMITTAL

TN: DT–99–28

To:	NRC Management Directives Custodians
Subject:	Transmittal of Directive 12.3, "NRC Personnel Security Program."
Purpose:	Directive and Handbook 12.3 have been revised to include the DEDM position and responsibilities, changes to position sensitivity criteria, and procedures for **NRC** contractor unescorted access to NRC facilities. Several revisions in the handbook were made to comply with Executive Order 12968, "Access to Classified Information," including eligibility for access to classified information, conditions for reinstatement of access, circumstances affecting eligibility for access to classified information, determination of eligibility, access for dual citizens and aliens, and the investigation and reinvestigation programs.
Office and Division of Origin:	Office of Administration
Contact:	Leigh Chase, 301–415–6541
Date Approved:	November 6, 1992 **(Revised: November 17, 1999)**
Volume:	12 Security
Directive:	12.3, "NRC Personnel Security Program."
Availability:	Rules and Directives Branch Office of Administration David L. Meyer (301) 415–7162 or Jeannette P. Kiminas (301) 415–7086

NRC Personnel Security Program

Directive 12.3

Contents

Policy 1

Objectives 1

Organizational Responsibilities and Delegations of Authority 1

Commission 1
General Counsel. Office of the General Counsel (OGC) 2
Director, Office of International Programs (OIP) 2
Deputy Executive Director for Management Services (DEDM) 2
Director, Office of Administration (ADM) 3
Director, Office of Investigations (OI) 3
Director, Office of Human Resources (HR) 4
Office Directors and Regional Administrators 4
Director, Division of Facilities and Security (DFS), ADM 5

Applicability 5

Handbook 5

Exceptions or Deviations 6

References 6

NRC Personnel Security Program Directive 12.3

Policy
(12.3-01)

It is the policy of the **U.S.** Nuclear Regulatory Commission to establish a personnel security program to ensure that determinations of an individual's eligibility for an NRC access authorization, employment clearance, unescorted access to nuclear power facilities; for access to unclassified Safeguards Information or to sensitive **NRC** information technology systems and data or unescorted access to NRC facilities; for the conduct of visits involving classified information; or for providing information to foreign regulatory assignees are accomplished in accordance with pertinent laws, Executive orders, management directives, and applicable directives of other Federal agencies.

Objectives
(12.3-02)

To provide effective controls to further protect classified and sensitive unclassified information.

Organizational Responsibilities and Delegations of Authority
(12.3–03)

Commission
(031)

- Grants access authorization and/or employment clearance to individuals for whom no report has been made to the NRC on their character, associations, and loyalty, provided that the Commission determines that this action is clearly consistent with the national interest. (a)

Commission
(031) (continued)

- Performs the Commission functions specified in 10 CFR Part 10 relative to personnel clearance cases subject to personnel security hearing procedures. (b)

General Counsel, Office of the General Counsel (OGC)
(032)

- Performs the functions assigned to the General Counsel under 10 CFR Part 10, including concurrence in the issuance of subpoenas. (a)
- Performs legal review of matters related to personnel security. (b)

Director, Office of International Programs (OIP)
(033)

Approves or disapproves the assignment of foreign regulatory employees to NRC after coordination with Division of Facilities and Security (DFS) and the office to which the person is temporarily assigned.

Deputy Executive Director for Management Services (DEDM)
(034)

- Performs the functions assigned to the DEDM under 10 *CFR* Part 10 including appointment of the NRC Hearing Counsel and the granting, suspension, denial, or revocation of **access** authorization in accordance with the requirements of 10 *CFR* Part 10. (a)
- Grants exemptions to 10 CFR Parts 25, "Access Authorization for Licensee Personnel," and 95, "Security Facility Approval and Safeguarding of National Security Information and Restricted Data," when a finding can be made that the requested exemption does not endanger the common defense and security, as authorized **by** SECY-80-387. (b)
- Performs the functions of the designated ***NRC*** Senior Agency Official, pursuant to the provisions of Section 6.l(a) of Executive Order (EO) 12968, "Access to Classified Information," to direct and administer the NRC's Personnel Security Program, including

Deputy Executive Director for Management Services (DEDM)
(034) (continued)

active oversight and implementation of continuing security education and awareness programs, to ensure that the order is effectively carried out. (c)

- Approves NRC's employment of individuals before the security investigation is completed, as required by Section 145b of the Atomic Energy Act of 1954, as amended (AEA), provided that the individual is not granted access to classified information, the requesting organization clearly demonstrates a need for the individual, and an affirmative recommendation is made by the Director, DFS, ADM. (d)

- Grants, under the authority in Section 145b, AEA, accesss to Restricted Data and other NRC classified information to designated members of Congress (no investigation to be conducted). This access, as authorized by SECY-81-291, applies to members of Congress serving on NRC Congressional Oversight Subcommittees. (e)

- Establishes, under the authority of Section 145g, AEA, standards and specifications in writing as to the scope and extent of investigations, the reports of which NRC will use to make the determination that permitting a person access to Restricted Data will not endanger the common defense and security. (f)

Director, Office of Administration (ADM)
(035)

- Performs the functions assigned to ADM under 10CFR Part 10. (a)

- Oversees the NRC personnel security program as carried out by the DFS, ADM. (b)

Director, Office of Investigations (OI)
(036)

Provides DFS any information developed or received in accordance with the OI/SEC agreement of February 1983.

Director, Office of Human Resources (HR)
(037)

Concurs in request for preappointment investigation waiver.

Office Directors and Regional Administrators
(038)

- Ensure that ***NRC*** employees, NRC contractor personnel, and any other personnel under their jurisdiction are cognizant of and comply with the provisions of this directive and handbook, as appropriate. (a)

- Ensure that ***NRC*** licensee and licensee-related personnel under their jurisdiction are cognizant of and comply with the personnel security provisions of 10 CFR Parts 10, 25, and 95. (b)

- Advise DFS of any information that indicates noncompliance with this directive and handbook or that is otherwise pertinent to the proper protection of classified interests, sensitive unclassified information, or ***NRC*** property. (c)

- Notify DFS of individuals under their jurisdiction who possess an access authorization or similar access approval, or for whom an access authorization or similar access approval has been requested, who are hospitalized or otherwise treated for an illness or mental condition that may cause defects in their judgment or reliability, and of any subsequent developments as required by this handbook. (d)

- Notify DFS of persons under their jurisdiction possessing access authorizations or similar access approval who are disabled for a prolonged period, who die, who for any other reason no longer require access authorization or similar access approval, require change of access authorization or similar access approval, or who are subject to any circumstance that may affect their continued eligibility for access authorization or access approval. (e)

- Report immediately to the Inspector General (IG) and DFS all alleged or suspected incidents of employee or contractor fraud, misconduct, unauthorized disclosure, or misuse of automated information systems. ***(f)***

Director, Division of Facilities and Security (DFS), ADM
(039)

- Plans, develops, establishes, and administers policies, standards, and procedures for the overall ***NRC*** personnel security program, including granting access authorization or similar access approval involving substantially derogatory information falling within 10 **CFR** 10.11 when the case has been favorably resolved through an interview or other investigation. (a)
- Administers the visitor control program which covers visits requiring access to classified information, the assignment of foreign regulatory employees to the NRC in coordination with the Office of International Programs, and the acceptance and issuance of security assurances to and from foreign governments. (b)
- Serves as the **NRC** central point of contact with the Federal Bureau of Investigation, the Office of Personnel Management, and other investigative agencies on ***NRC*** personnel security matters. (c)
- Recommends to the DEDM a preappointment investigation waiver. (d)

Applicability
(12.3–04)

This directive and handbook apply to all NRC employees, consultants, experts, panel members, applicants for employment, and other person designated by the DEDM as well as to all ***NRC*** contractors and subcontractors to whom they apply as a condition of a contract or a purchase order.

Handbook
(12.3-05)

Handbook 12.3 provides guidelines for personnel security, classified visits, and foreign assignees.

Exceptions or Deviations
(12.3–06)

Exceptions or deviations to this directive and handbook may be granted by DFS, except for those areas in which the responsibility or authority is vested solely with the Commission, the DEDM, or ADM and is nondelegable; or for matters specifically required by law, Executive order, or directive to be referred to other management officials.

References
(12.3-07)

Atomic Energy Act of 1954, as amended (42 U.S.C. 2011 et seq.).

***Code* of *Federal Regulations*-**

10 CFR Part 10, "Criteria and Procedures for Determining Eligibility for Access to Restricted Data or National Security Information or an Employment Clearance."

10 CFR Part 25, "Access Authorization for Licensee Personnel."

10 CFR Part 95, "Security Facility Approval and Safeguarding of National Security Information and Restricted Data."

32 CFR 147, 'Adjudicative Guidelines for Determining Eligibility for Access to Classified Information."

"Crimes and Criminal Procedures" (Title 18, United States Code).

Energy Reorganization Act of 1974, as amended (42 U.S.C. 5801 et seq.).

Executive Order 10450, "Security Requirements for Government Employment," April 27, 1953, as amended.

— 10865, "Safeguarding Classified Information Within Industry," February 20, 1960, as amended.

— 12958, "Classified National Security Information," April 17, 1995.

— 12968, 'Access to Classified Information," August 2, 1995.

Freedom of Information Act of 1966 *(5* U.S.C. 522).

"National Industrial Security Program Operating Manual **(NISPOM),"** Department of Defense.

References

(12.3–07) (continued)

NRC Management Directive-

3.1, "Freedom of Information Act."

3.2, "Privacy Act."

3.4, "Release of Information to the Public."

10.1, "Appointments, General Employment Issues, Details, and Position Changes."

11.1, "NRC Acquisition of Supplies and Services."

12.2, "NRC Classified Information Security Program."

NRC SECY-80-387, "Delegation of Authority to Grant Exemptions to 10 CFR Parts 25 and 95," August 15, 1980.

— 81-291, "Approval Under Section 145b of the Atomic Energy Act of 1954, as Amended, to Grant Access to Restricted Data and Other NRC Classified Information to Designated Members of Congress (No Investigation to be Conducted)," May 5, 1981.

NRC System of Records NRC-39, "Personnel Security Files and Associated Records-NRC."

Privacy Act of 1974, as amended (5 U.S.C. 552a).

"Suspension and Removal" (5 U.S.C. 7532).

NRC Personnel Security Program

Handbook 12.3

Contents

Part I

Access Authorization and Employment Clearance 1

Introduction (A) 1
Position Sensitivity Criteria (B) 1
" Q " Positions of a High Degree of Importance or Sensitivity (1) 1
Positions of a Critical and Sensitive Nature Require a "Q" Clearance (2) ... 2
Positions of High Public Trust Require an "L" Clearance (3) 2
"L" Positions of a Noncritical and Sensitive Nature (4) 3
Access Authorization Requests (C) 3
Employees (1) 3
Contractors (2) 4
Security Forms Packet (3) 4
Cancelled or Withdrawn Request (4) 5
Unescorted Access by NRC Contractors (D) 5
Sponsoring Office Responsibilities for Unescorted Access of NRC Contractors (1) 5
Unescorted Access of Nuclear Power Reactor Facilities (2) 6
Access to Unclassified Safeguards Information (SGI) by NRC Contractors (E) .. 8
Access to NRC Sensitive Information Technology Systems and Data by NRC Contractors (F) 8
IT Level I (1) 9
IT Level II (2) 10
Resolving Questions of Eligibility (3) 11
Continuous Unescorted Access to NRC Headquarters and Regional Office Facilities By NRC Contractor Employees and Others Not Otherwise Screened Under Sections C Through F Above (G) 11
Investigations (H) 13
Certification of "Q" and "L" Access Authorization (I) 14
Reopening of Cancelled Cases (J) 14
Preappointment Investigation Waiver With No Access to Classified Information (K) 14
Expedited Approval for Temporary Unescorted Access for NRC Employees, Including Inspectors and Resident Clerical Aides (L) 16
Extension and Transfer of Access Authorization (M) 16
Circumstances for Reinstatement (Reapproval) of Access Authorization (N) 17

Contents (continued)

Part I (continued)

Circumstances Affecting Eligibility for Access Authorization **(O)** **19**
Determination of Eligibility for Access Authorization (P) **20**
Interim Authorization for Access to Classified Information **(Q)** **20**
Access Authorization for Aliens and Dual Citizens (R) **21**
Data Report on Spouse (S) **22**
Reinvestigation Program (T) **22**
Termination of Access Authorization (U) **23**
Termination of Employment in the Interest of National Security (V) **25**
Termination of Access Approval **(W)** **25**

Part II

Control of Visits Involving Classified Information **26**

Introduction (A) **26**
General (B) **26**
Visits by NRC (C) **28**
NRC Employees **(1)** **28**
NRC Contractor or Subcontractor Personnel and NRC Consultants **(2)** **29**
Visits by Others (D) **30**
Personnel and Contractors of the Department of Defense (DOD) and the National Aeronautics and Space Administration (NASA) **(1)** ... **30**
Personnel, Contractors, and Subcontractors of the Department of Energy (DOE) **(2)** **31**
Employees. Contractors. and Subcontractors of Government Agencies Other Than DOD, NASA, or DOE **(3)** **31**
Members of Congress and Congressional Staff **(4)** **32**
Immigrant Aliens Admitted to the United States for Permanent Residence **(5)** **32**
Visits Involving Access to Sensitive Compartmented Information (SCI) (E) **32**
Visits by Foreign Nationals Sponsored by Foreign Governments or International Organizations (F) **33**
Visits to Foreign Governments or Activities by NRC Personnel (G) **33**
Records of Visit Requests (H) **34**

Contents (continued)

Part III

Assignment of Foreign Regulatory Employees to NRC **35**

Introduction (A) **35**
Activity Plans **(B)** **35**
Assignments (C) **35**
Background Check (D) **37**
Assignee Agreements (E) **37**
Security Plans **(F)** **38**
Assignee Responsibilities ***(G)*** **40**
Evaluation of Assignees (H) **40**

Exhibits

1 Due Process Procedures **41**
2 Format for a Request for a Preappointment Investigation Waiver **46**
3 Preemployment Screening and Section **145b** Processing Procedures for NRC Applicants **47**
4 Standard Operating Procedures for Preemployment Screening of NRC Applicants **48**
5 Expedited Temporary Unescorted Access Approval for NRC Employees. Including Inspectors and Resident Clerical Aides **50**
6 **"Q"** and **"L"** Reinvestigation Program Requirements **52**
7 Procedures for the Conduct of Hearings Under 5 U.S.C. **7532** **53**

Part I

Access Authorization and Employment Clearance

Introduction (A)

Procedures are given for meeting the requirements of the NRC personnel security program, which investigates and determines the eligibility of individuals for NRC access authorization and/or employment clearance, unescorted access to nuclear power facilities, access to unclassified Safeguards Information (SGI), access to sensitive NRC information technology systems and data, or unescorted access to NRC buildings. **(1)**

Personnel security and associated records maintained under the provisions of the NRC personnel security program are protected from public disclosure under the provisions of the Privacy Act of **1974,** as amended, and are subject to the routine uses specified for NRC System of Records **NRC-39,** "Personnel Security Files and Associated Records-NRC." **(2)**

Position Sensitivity Criteria (B)

These criteria determine whether a person in a particular NRC position requires a **"Q"** security clearance on the basis of a single-scope background investigation (SSBI) by the Federal Bureau of Investigation **(FBI),** or a "Q" or **High** Public Trust "L" on the basis of an SSBI by the Office of Personnel Management (OPM), or an **"L"** security clearance, as a minimum, on the basis of an access national agency check with inquiries **(ANACI).**

"Q" Positions of a High Degree of Importance or Sensitivity (1)

People in positions of a high degree of importance or sensitivity require an NRC **"Q"** access authorization based on an FBI **SSBI** pursuant to

Position Sensitivity Criteria (B) (continued)

***"Q"* Positions of a High Degree of Importance or Sensitivity (1)** (continued)

Section 145f of the Atomic Energy Act of 1954 (AEA), as amended. These positions include the following:

- The Chairman (a)
- An NRC Commissioner (b)
- Any other individual so designated by the Commission (Under this criterion, the Commission-designated Commissioners' assistants who have access to sensitive compartmented information.) (c)

Positions of a Critical and Sensitive Nature Require a "Q" Clearance (2)

People in critical and sensitive positions must have an ***NRC* "Q"** access authorization based on an OPM SSBI. Functions considered critical and sensitive have one or more of the following characteristics:

- Access to Secret or Top Secret Restricted Data or Top Secret National Security Information (a)
- Access to Confidential Restricted Data involving broad naval nuclear propulsion program policy or direction (e.g., preliminary safety analysis reports, final safety analysis reports, and amendments thereto) (b)

Positions of High Public Trust Require an "L" Clearance (3)

People in positions of **high** public trust require an "L" access authorization based on an **OPM** SSBI. The types of functions considered to be **of** high public trust include one or more of the following characteristics:

- Final approval of plans, policies, or programs that directly affect the overall operations and direction of the ***NRC*** (a)
- Responsibility for the planning, direction, and implementation of a computer security program; major responsibility for the direction, planning, and design **of** a computer system, including the hardware and software; or the capability to access a computer system during its operation or maintenance in such a way that could cause, or that has a relatively high risk of causing, grave damage; or the capability to realize a significant personal gain from computer access (b)

Position Sensitivity Criteria (B) (continued)

Positions of High Public Trust Require an "L" Clearance (3) (continued)

- Resident inspectors (c)
- Criminal investigators (d)
- Such other duties requiring high public trust as determined on an as-needed basis by the Deputy Executive Director for Management Services (DEDM) (e)

"L" Positions of a Noncritical and Sensitive Nature (4)

People in any NRC position not covered by Section **(B)(1), (2),** or **(3)** of this part require an NRC "L" access authorization based on an ANACI.

Access Authorization Requests (C)

Employees (1)

Access authorizations ("Q" or "L") for NRC employees, applicants for NRC employment (i.e., anyone who has received an authorized conditional offer of employment), and NRC experts, panel members, and consultants must be requested from the Division of Facilities and Security (DFS), Office of Administration, on NRC Form **236,** "Personnel Security Clearance Request and Notification," by the employing division director or his or her designee. Requests for access authorization are submitted through the Office of Human Resources (HR) or the Regional Personnel Office (RPO), as appropriate. The Office of the Inspector General (OIG) requests are forwarded directly to DFS. Instructions are printed on the reverse side of the form. (a)

The NRC official (HR or regional designee) responsible for submitting NRC Form **236** to DFS with a completed security forms packet shall ensure that the information shown on the applicant's employment form is consistent with the information reflected in Part **1** of the Questionnaire for National Security Positions **(QSP,** Standard Form [SF] **86).** If the information is not consistent, an explanation and assessment should be furnished to DFS regarding the inconsistency. (b)

Access Authorization Requests (C) (continued)

Contractors (2)

Access authorizations for NRC contractors, subcontractors, or other individuals who are not NRC employees (e.g., other Government agency personnel) may be requested on NRC Form 237, "Request for Access Authorization." The requester must forward this form to DFS or, if otherwise indicated, to the approving official of the NRC office sponsoring the activity that requires NRC access authorization. Instructions are printed on the reverse side of the form. (a)

At those contractor facilities at which ***NRC*** is not the cognizant security authority (CSA), access authorizations will be requested following the procedures of the CSA. (b)

Security Forms Packet (3)

Unless otherwise indicated, each request for access authorization must be accompanied by a properly completed security forms packet consisting of—(a)

- SF 86, QSP (Part 2 of the QSP is the privacy portion and is to be placed in the sealed envelope, NRC Form E-1, provided to the respondent. The NRC will maintain the privacy of the information provided on this form, Parts 1 and 2.) (i)
- Two applicant fingerprint cards (SF 87 for Federal employee applicants or FD 258 for contractors) (ii)
- NRC Form 176, "Security Acknowledgment" (iii)
- Two copies of Optional Form (OF) 612, "Optional Application for Federal Employment"; SF 171, "Application for Federal Employment" (6/88 or subsequent version); or equivalent for NRC applicants (iv)
- Related forms when so specified in the accompanying instructions (i.e., NRC Form 254) (To prevent errors and omissions that may delay consideration of a request, detailed instructions for completing the security forms packet, contained in NRC Form 254, should be followed carefully. Further instructions or guidance may be obtained from DFS.) (v)
- NRC Form 89, "Photo-Identification Badge Request" (for NRC employees, consultants, and contractors) (vi)

Access Authorization Requests (C)

Security Forms Packet (3) (continued)

DFS will return requests for access authorization to requester if—(b)

- All security forms are not completed and signed as required. (i)
- The printed content of the security or release form is altered. (ii)
- Required information is not provided. (iii)
- The forms are illegible. (iv)
- The "Authorization for Release of Information" on the SF 86 is not signed. (v)

Information entered on the forms in the security forms packet will be used in conjunction with any other relevant information to determine a person's initial or continuing eligibility for an access authorization, an employment clearance, unescorted access to nuclear power facilities, access to SGI, or access to sensitive NRC information technology systems and data. (c)

Cancelled or Withdrawn Request (4)

When a request for an applicant's access authorization or similar access approval is to be withdrawn or cancelled, DFS should be notified immediately by telephone so that the investigation may be promptly discontinued. The notification should contain the full name of the individual, the date of the request, and the type of access authorization or similar access approval request being cancelled. Telephone notifications must be promptly confirmed in writing to DFS.

Unescorted Access by NRC Contractors (D)

Sponsoring Office Responsibilities for Unescorted Access of NRC Contractors (1)

The *NRC* sponsoring office shall decide whether performance under an *NRC* contract will involve unescorted access to nuclear power facilities, access to nuclear power reactor unclassified SGI, access to *NRC* sensitive information technology systems and data, or unescorted access to NRC headquarters or regional office facilities. For these contracts, the sponsoring office shall-

Unescorted Access by NRC Contractors (D) (continued)

Sponsoring Office Responsibilities for Unescorted Access of NRC Contractors (1) (continued)

- Check "yes" for security requirements and insert one of the following statements in the appropriate block on the NRC Form 400, "Request for Procurement Action (RFPA)": (a)
  - "This contract requires unescorted access to nuclear power facilities by contractor employees," or "This contract requires contractor access to nuclear power reactor unclassified SGI, or "This contract requires access to NRC sensitive information technology systems and data." (i)
  - "This contract requires continuous unescorted access (in excess of **30** days or more) to NRC headquarters or regional office facilities, or otherwise requires NRC photo identification or keycard badges." (ii)
- Include an NRC Form **187,** "Contract Security and/or Classification Requirements," according to the requirements of Management Directive (MD) **11.1,** "NRC Acquisition of Supplies and Services," with the appropriate blocks in Section ***5*** of the form completed. (b)

Unescorted Access of Nuclear Power Reactor Facilities (2)

Individual contractors requiring access will be approved for unescorted access to protected and vital areas of nuclear power facilities in accordance with the following procedures:

- Temporary Approval (a)

  Temporary approvals may be obtained by two methods:

  - For the **first method,** the contractor shall submit to DFS through the NRC project officer the following information: (i)
    - A completed personnel security forms packet, including an **SF 86 QSP** *(a)*
    - Copies of the contractor's 5-year employment and education history checks, including verification of the highest degree obtained *(b)*
    - **A** reference from at least one additional person not provided by the individual ***(c)***

Unescorted Access by NRC Contractors (D) (continued)

Unescorted Access of Nuclear Power Reactor Facilities (2) (continued)

- **Results** of the psychological evaluation (d)
- A signed copy of *NRC* Form 570, "Access Authorization Acknowledgement" (The contractor employee's signature indicates that he or she understands his or her responsibility to report to NRC any information bearing on **his** or her continued eligibility for access authorization as specified in 10 CFR 10.11.) ***(e)***
- A certification that the contractor has found **all** checks acceptable **(f)**
- In limited cases, as determined by the sponsoring office, a copy **of** the contractor's 1-year employment check, along with items (D)(2)(a)(i)(a) and ***(c)*** through **(f)** of this part (g)

– DFS will conduct criminal history and credit checks and hold a security assurance interview **with** the contractor employee as specified in the above items. On the basis of the result of these checks, DFS will determine the contractor employee's eligibility for temporary access and will indicate "objection" or "no objection" to the sponsoring office, pending completion of the required background investigation. (ii)

– For the **second method,** the contractor employee will be fingerprinted by the utility and the individual will be subject to the utility's access authorization program. (iii)

- Final Approval (b)

Final access approval will be granted after—

– The required investigation on the individual has been completed and is satisfactory, resulting in ***NRC's*** endorsement of the individual's unescorted access at all nuclear facilities for the life of the contract. (i)

– The contractor has obtained unescorted access authorization (other than temporary access) at the specific facility through that utility's access authorization program. (ii)

– The individual possesses a valid Government-issued clearance as verified by DFS. (iii)

Unescorted Access by NRC Contractors (D) (continued)

Unescorted Access of Nuclear Power Reactor Facilities (2) (continued)

- Resolving Questions of Eligibility (c)

The investigation described in Section (D)(2)(b)(i) of this part may involve an ANACI or other investigation as DFS deems necessary. Any question regarding the contractor employee's eligibility for unescorted access to protected or vital areas of nuclear power facilities will be resolved in accordance with the provisions specified in Exhibit 1 of this handbook.

Access to Unclassified Safeguards Information (SGI) by NRC Contractors (E)

The NRC sponsoring office shall decide whether performance under an NRC contract will involve access to nuclear power reactor SGI. This access may require a national agency check (NAC) or other investigation as DFS deems necessary. Any question regarding the contractor employee's eligibility for access to nuclear power reactor SGI will be resolved in accordance with the provisions specified in Exhibit 1 of this handbook. Based on the review of the applicant's security forms by DFS and/or the receipt of adverse information by NRC, the individual may be denied access to nuclear power reactor SGI until a final determination of his or her eligibility for access is made under the provisions specified in Exhibit 1 of this handbook. While DFS is processing new contractor employees for access to nuclear power reactor SGI, access may be granted under licensee programs.

Access to NRC Sensitive Information Technology Systems and Data by NRC Contractors (F)

The Executive Director for Operations (EDO) approved the sensitivity criteria to be used in determining whether individual contractor employees shall require information technology (IT) Level I or II approval for access to NRC sensitive information technology systems and data. An IT Level I approval shall require a limited background investigation (LBI) by OPM and an IT Level II approval shall require, as a minimum, an ANACI by OPM. Dual citizens (United States citizens who are also a citizen of another country) and immigrant aliens and foreign nationals may be processed for IT Level I and II if investigative

Access to NRC Sensitive Information Technology Systems and Data by NRC Contractors (F)(continued)

coverage can be obtained for the immediate 10-year retrospective period. Only for these categories will an LBI be required for an IT Level 11.

IT Level I (1)

IT Level I involves responsibility for the planning, direction, and implementation of a computer security program; major responsibility for the direction, planning, and design of a computer system, including the hardware and software; or the capability to access a computer system during its operation or maintenance in such a way that could cause or that has a relatively high risk of causing grave damage; or the capability to realize a significant personal gain from computer access. Such positions may involve-

- Responsibility for the development and administration of agency computer security programs, including direction and control of risk analysis and/or threat assessment (a)
- Significant involvement in life-critical or mission-critical systems (b)
- Responsibility for the preparation or approval of data for input into a system that does not necessarily involve personal access to the system but with relatively high risk for causing grave damage or realizing significant personal gain (c)
- Relatively high risk assignments associated with or directly involving the accounting, disbursement, or authorization for disbursement from systems of either—(d)
  - Dollar amounts of **$10** million per year or greater (i)
  - Lesser amounts if the activities of the individual are not subject to technical review by higher authority at the IT Level I to ensure the integrity of the system (ii)
- Positions involving major responsibility for the direction, planning, design, testing, maintenance, operation, monitoring, and/or management of systems hardware and software (e)
- Other positions that involve relatively high risk for causing grave damage or realizing significant personal gain **(f)**

Access to NRC Sensitive Information Technology Systems and Data by NRC Contractors (F) (continued)

IT Level II (2)

All other IT positions. (a)

Individual contractor employees requiring access will be approved for access in accordance with the following procedures. (b)

- Temporary Approval (i)
  - The contractor shall submit a completed personnel security forms packet, including an **SF** 86 **QSP** to DFS through the ***NRC*** project officer. ***(a)***
  - The project officer shall forward the completed security forms packet to DFS together with a written request identifying whether the contractor employee shall be processed for IT Level I **or** II approval and the specific criterion(ia) that applies. *(b)*
  - DFS will conduct criminal history and credit checks and will hold a security assurance interview with the individual. **(c)**
  - On the basis of the results of these checks, DFS will determine the contractor employee's eligibility for temporary access and will indicate approval or disapproval to the sponsoring office, pending completion of the required background investigation and final approval for IT Level I **or II** access. ***(d)***
- Final Approval (ii)
  - Final access approval will be granted after the required investigation on the contractor employee has been completed and is satisfactory, resulting in the contractor employee's approval for IT Level I or **II** access. ***(a)***
  - **DFS** will notify the sponsoring office of final approval. *(b)*

Access to NRC Sensitive Information Technology Systems and Data by NRC Contractors (F) (continued)

Resolving Questions of Eligibility (3)

Any question regarding the contractor employee's eligibility for IT Level I or **II** approval will be resolved in accordance with the due process procedures (Exhibit **1** of this handbook). On the basis of DFS's review of the contractor employee's security forms and/or the receipt of adverse information, the contractor employee may be denied access to ***NRC*** sensitive information technology systems and data until a final determination of eligibility for access is made under the provisions of due process.

Continuous Unescorted Access to NRC Headquarters and Regional Office Facilities By NRC Contractor Employees and Others Not Otherwise Screened Under Sections C Through F Above (G)

The ***NRC*** sponsoring office shall decide whether performance under an ***NRC*** contract, interagency agreement, memorandum of understanding, or similar agreement, will involve continuous unescorted access (in excess of **30** or more days) or otherwise requires ***NRC*** photo identification or keycard badge to ***NRC*** headquarters buildings and regional office facilities by ***NRC*** contractor employees, or by other individuals not covered by ***NRC*** contracts (e.g., vendors, health unit personnel). This access will require limited background checks (i.e., criminal history checks, conducted by the General Services Administration **[GSA]).** For these contractual or other similar arrangements or agreements, the sponsoring office shall include an ***NRC*** Form 187 with Section 5F checked. **(1)**

Individual contractor employees or other individuals requiring access will be approved for continuous unescorted access in accordance with the following procedures: (2)

Continuous Unescorted Access to NRC Headquarters and Regional Office Facilities By NRC Contractor Employees and Others Not Otherwise Screened Under Sections C Through F Above (G) (continued)

- Temporary Approval (a)

  The contractor shall submit the following information to DFS through the ***NRC*** headquarters or regional project officer: a completed GSA Form 176, "Statement of Personal History," and two FD-258s, "Fingerprint Chart," and ***NRC*** Form 89, "Photo Badge Request." (i)

  On the basis of the DFS review of the applicant's security forms and/or NRC's receipt of adverse information, DFS will determine the individual's eligibility for temporary access and will indicate approval or disapproval to the sponsoring office, pending completion of the required criminal history checks and final approval by GSA. (ii)

- Final Approval (b)

  Final continuous unescorted access approval will be granted under one of the following conditions:

  - After completion and approval of the required GSA investigation, indicated in Section (G)(2)(a) of this part, resulting in GSA's endorsement **of** the individual's unescorted access to ***NRC*** facilities (i)
  - **As** determined by DFS, the individual possesses a valid NRC/Government-issued clearance or has previously received final security approval under one of DFS' various screening programs (ii)

- Recertification (c)

  This approval is valid for **3** years from the date of the notification letter to the requester, provided that the individual remains employed under the contract, agreement, or similar arrangement. In accordance with GSA requirements, each individual who is approved for unescorted building access must be recertified every **3** years from the date of the initial approval and each subsequent recertification. (i)

Continuous Unescorted Access to NRC Headquarters and Regional Office Facilities By NRC Contractor Employees and Others Not Otherwise Screened Under Sections C Through F Above (G) (continued)

Ninety days before the expiration of the initial approval, and each subsequent recertification, the contractor will submit a GSA Form 176, "Statement of Personal History," and two FD-258s to DFS, through the NRC headquarters or regional project officer, for each individual who requires recertification. With timely application and in the absence of any adverse information, the individual will maintain unescorted access pending recertification. If the contractor fails to submit a timely application, unescorted access approval will expire at the end of the 3-year period and the individual will be denied admittance to NRC space. (ii)

- Resolving Questions of Eligibility (d)

  Any questions regarding the individual's eligibility for continuous unescorted access to NRC facilities on the basis of the GSA investigation will be resolved directly between the individual and GSA.

A contractor employee or other individual requiring unescorted access shall not be provided unescorted access to NRC facilities until he or she is approved for temporary or final access in accordance with these procedures. (3)

Investigations (H)

The hiring or employing office, in concert with HR, shall determine the position sensitivity for NRC employees, applicants for employment, consultants, experts, and panel members, using the criteria specified in Section (B) of this part, before requesting access authorization for these individuals. The access authorization or similar access approval level or type of investigation required for NRC contractor and subcontractor employees will usually be determined on the basis of their classified access requirements, their need for unescorted access to nuclear power facilities, their access to SGI, access to sensitive NRC information technology systems and data, or unescorted access to NRC headquarters or regional office facilities. (1)

Investigations (H) (continued)

In lieu of an OPM investigation and report, NRC may accept an investigation and report not more than 5 years old for **"Q"** access authorization (or **"L"** access authorization for a position of **high** public trust) and not more than 10 years old for **an "L"** access authorization on the character, associations, and loyalty of an individual from another Government agency that conducts personnel security investigations, provided that an access authorization has been granted to the individual by another Government agency on the basis of such **an** investigation and report. (2)

Certification of "Q" and "L" Access Authorization (I)

An NRC ***"Q"*** access authorization and an NRC "L" access authorization for positions of high public trust may be granted on the basis of a current Top Secret or **"Q"** access authorization certified by another Government agency if the supporting **SSBI** investigation is not more that 5 years old. An NRC "L" access authorization for other than high public trust positions may be granted on the basis of a current Secret or "L" access authorization certified by another Government agency if the supporting ANACI or national agency check with law and credit (NACLC), as appropriate, is not more than 10 years old. ***An*** up-to-date security forms packet may be required before certification can be granted.

Reopening of Cancelled Cases (J)

For security clearance processing requests that are cancelled before the investigation is completed, and more than 90 days have elapsed since the security forms originally submitted were signed, the individual will be required to update a copy of the forms, if necessary, and resign and date the forms so they may be submitted for investigation.

Preappointment Investigation Waiver With No Access to Classified Information (K)

The Deputy Executive Director for Management Services (DEDM) is authorized to approve the employment of an individual by the NRC before completion of the security investigation and the reports required by Section 145b of the AEA. This authority may not be

Preappointment Investigation Waiver With No Access to Classified Information (K) (continued)

redelegated and is limited to situations in which the individual will not have access to classified information. Also, there must be an affirmative recommendation from the Director, DFS, and a clear need shown by the requesting organization to use the services of that individual during the required investigation. **(1)**

A request for a preappointment investigation waiver (Exhibit **2)** must be forwarded to HR for evaluation and processing, with the exception of waivers involving OIG. If concurred in by HR and DFS, HR will send the request to the DEDM for approval or disapproval. OIG will forward a request for a preappointment investigation waiver to DFS. If concurred in by DFS, OIG may send the request directly to the DEDM for approval or disapproval. All waivers must—(2)

- Be requested by the office director or the deputy office director for headquarters personnel or by the regional administrator or deputy regional administrator for regional personnel (a)
- Be justified by indicating that a serious delay or interference to an essential **NRC** operation or program will occur unless the individual is employed as soon as possible (b)
- Indicate that administrative controls will be established to ensure the individual will not have access to classified information until the appropriate access authorization is granted (c)
- Be concurred in by the Director or Deputy Director, HR, the Director or Deputy Director, DFS, and if regional personnel are involved, the Regional Personnel Officer (d)

HR and DFS shall process all Section 145b requests in accordance with the procedures specified in Exhibit **3** of this handbook. HR or the RPO, when applicable, must provide DFS with the results of pre-employment checks conducted on **NRC** applicants who are being considered for employment under Section 145b.**(3)**

Preappointment Investigation Waiver With No Access to Classified Information (K) (continued)

An exception to personnel reference checking for consultants or experts may be recommended to the Director, HR, by the office director or the regional administrator in those cases in which the consultant or expert is known to be highly regarded and respected in the professional community. This recommendation must be reflected in the Section 145b request (Exhibit **2). (4)**

In the case of students being considered for temporary summer appointments, personal reference checking must be conducted in accordance with the procedures specified in Exhibit 4. (5)

Expedited Approval for Temporary Unescorted Access for NRC Employees, Including Inspectors and Resident Clerical Aides (L)

When requests for approval for unescorted access to nuclear power facilities by **NRC** employees are received, including those from inspectors and resident clerical aides, the procedures specified in Exhibit 5 must be followed. When the need for temporary access is known at the time the Section 145b request **is** prepared, that need must be documented in the Section 145b request (Exhibit **2).**

Extension and Transfer of Access Authorization (M)

An extension of an access authorization by DFS permits an individual who possesses an active **NRC** access authorization in connection with a particular employer or activity to have concurrent access to classified information at a level comparable to or lower than that already authorized. (1)

Transfer of an access authorization is the termination of an individual's access authorization from one employer or activity while at the same time activating the access authorization at another employer or activity. (2)

Extension and Transfer of Access Authorization (M) (continued)

The requester should ensure that requests to DFS for extension or transfer of access authorization contain the full name, social security number, and date of birth of the individual, in addition to the level of access authorization requested. At the discretion of DFS (as, for example, in the case of significant changes since execution of the last **QSP),** a new security forms packet may be required. In all cases involving the extension or transfer of an access authorization to a position certified as being **of a high degree of importance or sensitivity,** a new security forms packet will be required. **(3)**

Circumstances for Reinstatement (Reapproval) of Access Authorization (N)

Where access has been terminated because an individual no longer has need for access and a new need for access arises, access eligibility up to the same level shall be reapproved without further investigation provided the last investigation was completed within the past ***5*** years; he or she has remained employed with the same employer during the period in question; the individual certifies in writing through the completion of a new **SF** 86 or by updating and resigning a copy of his or her most recent **SF** 86 that there has been no change in the relevant information provided by the individual for the last investigation; and there is no information that would tend to indicate the individual may no longer satisfy the standards established by EO 12968 for access to classified information. (1)

Access eligibility shall be reapproved for individuals who were determined to be eligible on the basis of a favorable adjudication of an investigation completed within the prior ***5*** years and who have been retired or otherwise separated from United States Government employment for not more than 2 years, provided there is no indication, through the completion of a new **SF** 86 or by updating and resigning a copy of his or her most recent **SF** 86, the individual may no longer satisfy the standards of information provided by the individual for the last background investigation, and an appropriate record check reveals no unfavorable information. (2)

Circumstances for Reinstatement (Reapproval) of Access Authorization (N) (continued)

An access authorization may be reinstated at the same or lower level if no significant changes are known to have occurred since the date of the SF **86** used for the current investigation. When new security forms are not required, requests for reinstatements will contain the full name, social security number, and date of birth of the individual to establish positive identification. A new "Security Acknowledgment" will be obtained in all cases. **(3)**

A supplemental investigation will normally be requested before reinstatement when—(4)

- More than 5 years has elapsed since the previous investigation or the individual has not remained employed with the same employer during the time period in question. (a)
- More than 2 years have elapsed since the access authorization of the individual has been terminated as a result of separation or retirement from **U.S.** Government employment. (b)

When the reinstatement involves the assignment of an individual to a position **of a high degree of importance or sensitivity** and the previous investigation was conducted by a Government agency other than the FBI, a new security forms packet will be forwarded to the FBI for investigation. The Chief, Personnel Security Branch (PERSEC), DFS, may authorize the reinstatement of access authorization before the report of the new investigation is received from the FBI. ***(5)***

When the reinstatement involves an individual who falls within the scope of the reinvestigation program, a new security forms packet will be obtained and the case will concurrently be processed for reinvestigation. The Chief, PERSEC, may authorize the reinstatement of access authorization before the reinvestigation report is received. **(6)**

Circumstances Affecting Eligibility for Access Authorization *(O)*

When a person who possesses or is being processed for NRC access authorization, unescorted access to nuclear power facilities, access to SGI, or access to sensitive NRC information technology systems and data, or unescorted access to NRC headquarters or regional office facilities is hospitalized or otherwise treated for an illness or mental condition that may cause a defect in the person's judgment or reliability, the person's employer (i.e., in the case of an NRC employee, the employee's office director, regional administrator, or other designated official) shall promptly report the circumstances to the Director, DFS. (1)

In the case of contractor personnel, the circumstances must promptly be reported to the Director, DFS, by the contracting officer, the security officer, or other person ***so*** designated. (2)

The reporting requirements of Sections (O)(1) and (2) of this part do not relieve an individual from the requirement to report to DFS his or her arrest as required by the QSP (SF 86), the security acknowledgment (NRC Form 176), or other form signed by the individual. The arrest must be reported within 10 workdays. (3)

Other circumstances that may affect a person's initial or continued eligibility for NRC access authorization, employment clearance, unescorted access to nuclear power facilities, access to SGI, or access to sensitive NRC information technology systems and data are listed in 10 CFR 10.11. These matters must also be promptly reported to the Director, DFS, by the person's designated employment official. (4)

Individuals are encouraged and expected to report any information that raises doubts as to whether another individual's continued eligibility for access to classified information is clearly consistent with the national security. ***(5)***

NRC employees and designated management officials are encouraged to seek information and assistance available from the NRC Employee Assistance Program Manager concerning issues that may affect an individual's eligibility for security clearance, including sources of assistance about financial matters, mental health, and substance abuse. NRC contractor personnel and others may seek assistance from similar financial, health, and substance abuse organizations in the local community. (6)

Determination of Eligibility for Access Authorization (P)

Except as provided for in Section (R) of this part, an NRC **"L"** or **"Q"** access authorization shall be granted only to employees and contractors who are United States citizens for whom an appropriate investigation has been completed and whose personal and professional history affirmatively indicates loyalty to the United States, strength of character, trustworthiness, honesty, reliability, discretion, and sound judgment, as well as freedom from conflicting allegiances and potential for coercion, and willingness and ability to abide by regulations governing the use, handling, and protection of classified information. The determination of eligibility for access authorization will be consistent with **5** U.S.C. **7532** or 10 CFR Part 10. The determination of eligibility for unescorted access to nuclear power facilities, access to **SGI,** or access to sensitive NRC information technology systems and data will be made in accordance with the provisions of Exhibit **1** of this handbook. **(1)**

Applicants for NRC access authorization will be required to sign an **SF 312,** "Classified Information Nondisclosure Agreement." **(2)**

Interim Authorization for Access to Classified Information (Q)

Only the Commission may grant an interim access authorization for access to Restricted Data. **(1)**

Requests for interim access authorization must be forwarded to DFS in the same manner as requests for access authorization and must include the forms and information specified in Section (C) of this part. These requests also must include a justification from the NRC sponsoring office that a serious delay or interference in an operation or project essential to an NRC program may be experienced unless the designated individual is granted immediate access to classified information. **(2)**

HR or the RPO, as appropriate, must provide DFS with the results of the preemployment checks on NRC applicants who are being considered for interim access authorization (see Exhibit **4** for the scope of the required preemployment checks). **(3)**

If DFS's evaluation of the information developed on an applicant is unfavorable, DFS will inform the requester of its recommendation in the matter and, if applicable, HR. **(4)**

Access Authorization for Aliens and Dual Citizens (R)

A dual citizen, that is, a United States citizen who is also a citizen of another country, may be processed for a "Q" or an "L" access authorization when the need for access authorization is adequately supported and investigative coverage can be obtained for the immediate 10-year retrospective period. ***As*** provided for in EO 12968, where there are compelling reasons in furtherance of the ***NRC's*** mission, immigrant aliens and foreign national employees who possess a special expertise may, in the discretion of the Director, DFS, be granted an ***NRC*** "L" or "Q" access authorization with access to classified information limited to the specific programs, project, contracts, licenses, certificates, or grants for which there is a need for access. Such individuals shall not be eligible for access to any greater level of classified information than the United States Government has determined may be releasable to the country of which the subject is currently a citizen, and such limited access may be approved only if the prior 10 years of the subjects life can be appropriately investigated.(1)

An interview with the applicant will normally be conducted and include the applicant's - (2)

- Statement and disclosure of national allegiance (a)
- Intent as to permanent residence in the United States (b)
- General attitude toward the United States vis-a-vis the country of the applicant's current citizenship (c)
- For dual citizens, eligibility and intention to maintain dual citizenship (d)
- Previous civilian or military service with a foreign government (e)
- Family or other relatives abroad or employed by a foreign government **(f)**
- The names and addresses of United States citizens who can furnish information as to the applicant's background and activities outside the United States ***(g)***

A verbatim transcript or detailed ***summary*** of the interview will be maintained and provided to the applicant upon request. **(3)**

Access Authorization for Aliens and Dual Citizens (R)(continued)

If DFS concludes that adequate support exists to initiate the investigation, the pertinent record will be forwarded to the investigation agency. *An* SSBI will be required for an "L" access authorization. (4)

If DFS concludes that the case is not suitable for further processing, the *NRC* sponsor (e.g., HR) will be informed and given advice as to whether the objection to processing can be resolved by submission of further information, documentation, or testimony. (5)

Data Report on Spouse (S)

Applicants for *NRC* access authorization, unescorted access to nuclear power facilities, access to SGI, or access to sensitive *NRC* information technology systems and data whose spouses are aliens, or who marry after they have submitted a **QSP,** must furnish DFS with two copies of *NRC* Form 354, "Data Report on Spouse."

Reinvestigation Program (T)

The *NRC* reinvestigation program **is** designed to ensure the continued eligibility for access authorization of individuals employed in the *NRC* program. The program applies to all those who possess "Q" or "L" access authorization, including *NRC* employees, consultants, experts, panel members; former senior *NRC* officials who retain their clearances after terminating their employment when continued access to classified information is required in the conduct of the agency's activities; congressional staff members cleared by *NRC*; employees and consultants of *NRC* contractors; and agents of *NRC*. DFS must reevaluate the continued eligibility of those individuals cleared at the "Q level not to exceed every 5 years. The eligibility of individuals cleared at the "L" level who are in positions of **high** public trust must be reevaluated not to exceed 5 years. *All* other individuals cleared at the "L" level (e.g., a regular "L" must be reevaluated not to exceed 10 years. (See Exhibit **6** for "Q" and "L" reinvestigation requirements.) **(1)**

Reinvestigation Program (T) (continued)

Each year, **DFS** will provide NRC office directors and regional administrators, or their designees, with the names of the individuals in their offices who are to be reinvestigated and the dates by which the individuals are to complete the security forms packet. DFS will advise former senior NRC officials who have retained their NRC security clearances, congressional staff members, and contractor organizations directly. DFS will provide each individual to be reinvestigated with a security forms packet and advise him or her of the due date. (2)

Each individual must complete the security forms packet and return it to his or her office or regional contact in a sealed envelope by the specified date. The office director or the regional administrator, or their designee, must ensure that individuals complete and return security forms packets to them and that all completed and sealed security forms packets are returned to DFS by the specified date. Contractor personnel must return forms through their security office. If the contractor fails to submit forms by the specified date, the NRC security clearance for contractor personnel may be administratively terminated. (3)

Upon satisfactory completion of the investigation, DFS will provide certification to the appropriate personnel office for the individual's official personnel file or other appropriate record. **(4)**

Termination of Access Authorization (U)

Access authorization will be terminated and a security termination statement (NRC Form 136) must be signed when—(1)

- ***An*** individual is separated from employment with the NRC. (a)
- In the case of a non-NRC employee, an individual is separated for a period of 60 days or more from activities for which he or she was granted an access authorization. (b)
- Access authorization is no longer required. (c)

Upon the voluntary or involuntary separation (e.g., death) from employment of a person who holds an NRC access authorization, the employing office at headquarters or the regional office or facility (e.g., an NRC contractor) must as a minimum, when applicable to persons being separated—(2)

Termination of Access Authorization (U)(continued)

- Provide prompt notification of the termination of employment to DFS and headquarters or the regional office, if other than the employing office, as applicable (a)
- Ensure that all classified and sensitive unclassified documents charged to the person are accounted for and properly disposed of (b)
- Arrange for the recovery of badges, passes, and other forms of official identification and their return to the responsible security office or ***NRC*** official (in the case of ***NRC*** employees) (c)
- Arrange for the person's name to be removed from all access and mailing lists, especially those involving classified **or** sensitive unclassified information (d)
- Ensure that combinations are changed of any repositories to which the person had access (e)
- Arrange for the person's name to be removed from access permissions to critical or sensitive areas, such as telephone closets and computer rooms **(f)**
- Arrange for the deactivation of the person's formal access permissions to all IT systems from mainframes to desktops as well as Internet working systems such as the local area network. (g)
- Arrange for the deactivation, expiration, or removal of the person's user IDs; if the user's ID and password are shared by others, the password should be changed immediately (h)
- Arrange for the deactivation, expiration, or removal of the person's external communications login ID (i)

Upon completion of a security termination statement—(3)

- The signed copy of the security termination statement must be forwarded to DFS. DFS will retain the statement in the employee's personnel security file. (a)

Termination of Access Authorization (U) (continued)

- If a security termination statement is used when an individual's association with a particular contract, agreement, or facility is terminated, but the NRC access authorization is to remain active, the following wording is suggested to modify the introductory paragraph of the statement: (b)

  "I make the following statement relating to the termination of my access authorization granted by the Nuclear Regulatory Commission in connection with my work, or my association with *(name of contractor; party to agreement of facility)*. My NRC access authorization will remain active in connection with other interests."

Disability **(4)**

In the case of the disability of a person when it is apparent that the disability will render the individual unable to perform his or her duties for at least 6 months, prompt notification must be made to DFS and measures similar to those specified in Section (U)(2)(b) through (i) of this part must be employed.

Termination of Employment in the Interest of National Security (V)

The DEDM may suspend or remove an employee when suspension or removal is considered to be in the interest of national security in accordance with 5 U.S.C. 7532. (1)

The criteria set forth in 10 CFR 10.11 must be used to determine whether an action should be taken under 5 U.S.C. 7532. (2)

When a hearing is held under 5 U.S.C. 7532, the ***NRC's*** "Procedures for the Conduct of Hearings Under 5 U.S.C. 7532" (Exhibit 7) must be used. (3)

Termination of Access Approval (W)

The **NRC** sponsoring office must immediately notify **DFS** in writing when a contractor employee no longer requires unescorted access to nuclear power facilities, access to **SGI,** access to sensitive NRC information technology systems and data, or unescorted access to NRC headquarters or regional office facilities.

Part II

Control of Visits Involving Classified Information

Introduction (A)

Standards and procedures are given for the protection of classified information involved in the course of visits to NRC, or visits by NRC employees and NRC contractors to other Government agencies and contractors.

General (B)

Before disclosing classified information to any visitor, individuals must confirm the visitor's identity, need-to-know, and level of access authorization. **(1)**

NRC or contractor officials (e.g., supervisors) must ensure that visit requests are submitted early enough for timely processing and notification of the person or facility to be visited. (2)

Continuing visit approval for **1** year or less may be granted for repeated visits to NRC, the Department of Energy (DOE), or other facilities. **A** single visit request form may be used if the repeated visits are to the same facility and involve the same individuals, the same level of classified information (e.g., Secret), and the same type of classified information (e.g., Restricted Data). **(3)**

Visit requests of an unusual or emergency nature for which timely notification cannot be given may be transmitted to the NRC Division of Facilities and Security (DFS), Office of Administration, by facsimile, teletype, or telephone. Telephone arrangements must be immediately confirmed with DFS in writing. Visit requests that are not in writing or that do not provide timely notification may not be accepted at some facilities. **(4)**

General (B) (continued)

Classified information must not be given to NRC employees or other individuals who possess an NRC red (no access) badge. (5)

Access to classified information other than that authorized in the visit request must not be granted, regardless of the level of access authorization stipulated for the visitor. ***(6)***

The NRC office, NRC contractor, or other NRC activity visited shall establish appropriate administrative controls over the movement of approved visitors to ensure that they are given access only to the classified information authorized. (7)

Neither classified nor unclassified naval nuclear propulsion information may be disclosed to individuals who are not United States citizens or to others not authorized access to this information. (8)

The NRC photo-identification badge will be accepted as authority for admission to DOE headquarters but is not accepted as authority for access to classified information. Similarly, the DOE photo identification badge will be accepted as authority for admission to NRC headquarters but may not be accepted as authority for access to classified information (see Section (D)(2) of this part). (9)

If appropriate, the visitor should confirm in advance with the facility to be visited that necessary approvals have been received. **(10)**

Access to Restricted Data requires a **"Q"** or **"L"** access authorization, depending on the classification level of the Restricted Data, except as provided in Section (D)(1) of this part. **(11)**

Requests for visits to NRC offices or divisions, except as indicated in Section (C)(1)(a) of this part, to NRC contractors, to other NRC facilities, or to other Government agencies involving classified information must be requested on NRC Form 277, "Request for Visit or Access Approval," or in an appropriate written request containing the following information: (12)

- Identity of each visitor, including full name, social security number, citizenship, date of birth, and organization with which affiliated (a)
- Specific information to which access is requested, including the classification level and type of information, for example, Restricted Data or National Security Information (b)

General (B) (continued)

- Access authorization level **("Q",** "L" Top Secret, Secret, or Confidential) and the need-to-know of each person certified by an appropriate official (c)
- Purpose of the visit (d)
- Name and location of facility(ies) to be visited (e)
- Anticipated dates of visit and names of persons to be visited (If a conference is involved, provide the date, place, and sponsor of the conference.) **(f)**
- Name, title of position, organization, and telephone number of the person who prepared the request (g)
- Requests for visits to NRC, NRC contractors, or other NRC facilities by individuals outside NRC should be sent to the following address: (h)

  U.S. Nuclear Regulatory Commission
  Chief, Personnel Security Branch
  Division of Facilities and Security
  Washington, D.C. 20555

Classified notes or other classified records must not be released to a visitor to take outside the facility without the express permission of the person visited. If the visit is in connection with a conference or other such activity, the express permission **of** the person responsible for the activity must be obtained. Also, records so released must be protected in accordance with Management Directive (MD) 12.2, "NRC Classified Information Security Program." (13)

Visits by NRC (C)

NRC Employees (1)

For visits to NRC headquarters and regional offices, a request for visit or access approval (NRC Form 277) is not necessary. The employee's NRC photo-identification badge will serve to identify the employee and the access authorization held. A blue badge signifies a **"Q"** access authorization and a yellow badge an **"L".** A red photo-identification badge signifies no access authorization has been granted to the employee. (a)

Visits by NRC (C) (continued)

NRC Employees (1) (continued)

For visits to NRC contractors, licensees and their related facilities, and to other Government agencies or their contractors, NRC employees should submit an NRC Form 277 to DFS at least 7 working days before the initial date of the visit. When acting as representatives of the Federal Government in their official capacities as inspectors, investigators, or auditors, NRC employees may visit a contractor or licensee facility, without furnishing advanced notification, provided these employees present appropriate NRC credentials upon arrival. (b)

Access to weapon data, sensitive nuclear material production information, inertial fusion data, advanced isotope separation technology, uranium enrichment technology, or naval nuclear propulsion information requires special processing and approval by DOE. For this reason, an NRC Form 277 should be submitted to DFS at least 15 working days before the initial visit date. (c)

For visits to facilities performing work on naval reactors for DOE, an NRC Form 277 should be received at least 15 working days before the initial visit date, especially for visits that do not involve inspections. (d)

A separate NRC Form 277 should be used for visits to a Government agency other than NRC, to DOE headquarters, and to DOE field or area offices having jurisdiction over the facilities and personnel being visited. (e)

NRC Contractor or Subcontractor Personnel and *NRC* Consultants (2)

For visits to facilities other than NRC, an NRC Form 277 or other written request for visit or access approval should be submitted to the NRC office or division sponsoring the contract, to the consultant or licensed activity to be visited for certification of the individual's need-to-know, and to DFS for verification of access authorization. The NRC sponsoring office or division should receive the visit request at least 15 working days before the initial date of the visit. Because of the limited number of firms that have classified contracts with NRC, the authority to certify the contractor employees clearance and need-to-know shall remain with DFS. At those contractor or licensee facilities at which NRC is not the cognizant security authority (CSA), the visit control procedures of the CSA shall be followed. (a)

Visits by NRC *(C)* (continued)

NRC Contractor or Subcontractor Personnel and *NRC* Consultants (2) (continued)

Requests to visit ***NRC*** offices should be submitted directly to DFS at least 10 working days before the initial date of the visit. (b)

Requests for visits to facilities performing work on naval reactors for. DOE should be received by the ***NRC*** sponsoring office or division at least 15 working days before the initial visit date. (c)

NRC consultants who plan to visit ***NRC*** employees directing or monitoring their consultant interests will not be required to submit an ***NRC*** Form 277. The person visited must confirm the ***NRC*** consultant's need-to-know and required access authorization level before classified information is disclosed to the visitor. (d)

Visits by Others (D)

Personnel and Contractors of the Department of Defense (DOD) and the National Aeronautics and Space Administration (NASA) (1)

For visits by personnel and contractors of DOD and **NASA** to ***NRC,*** ***NRC*** contractors, or other NRC facilities, an ***NRC*** Form ***277,*** a NASA Form 405, or a memorandum or teletype signed by or in the name of an official of the agency originating the request must be submitted to DFS for processing and approval by the ***NRC*** activity involved. (a)

DOD or Armed Forces personnel and contractors may be granted access to Restricted Data on the basis of an ***NRC*** **"Q"** or **"L"** access authorization or a DOD-certified access authorization (security clearance) approved by the ***NRC*** activity involved. (b)

NASA personnel or their contractors may be granted access to Restricted Data related to aeronautical or space activities on the basis of a NASA access authorization (security clearance). Access to Restricted Data not related to aeronautical and space activities will require an ***NRC*** **"Q"** or **"L"** access authorization, depending on the classification level of the Restricted Data. (c)

Visits by Others (D)(continued)

Personnel, Contractors, and Subcontractors of the Department of Energy (DOE) (2)

For visits by personnel, contractors, and subcontractors of DOE to NRC, NRC contractors, or other NRC facilities, a DOE Form DOE F 5631.20, an NRC Form 277, or a memorandum or teletype signed by or in the name of the appropriate DOE official should be transmitted to DFS. Verification of DOE access authorization and certification of need-to-know must be included in the visit request before NRC will process the request. (a)

Contractor personnel at DOE national laboratories who are engaged in contract work for the NRC should have DOE forward their visit requests for transmission to DFS. These requests verify their DOE access authorization to the NRC office administering the contract. (b)

Employees, Contractors, and Subcontractors of Government Agencies Other Than DOD, NASA, or DOE (3)

Restricted Data in the possession of the NRC, its contractors, or in NRC facilities must not be released to visitors from Government agencies or their contractors unless they have the appropriate ***NRC*** or DOE access authorization and the need for access has been properly certified. (a)

Classified information, other than Restricted Data, may be furnished to employees of agencies and their contractor or subcontractor personnel when they have the required access authorization and their need for access is confirmed by the **NRC** activity to be visited. (b)

For visits involving access to classified information, including Restricted Data, an ***NRC*** Form 277 or a memorandum or teletype signed by or in the name of an official of the requesting agency should be submitted to DFS for processing and approval by the NRC activity involved. (c)

If authorized by the Director, DFS, representatives of other agencies (e.g., the FBI or OPM) acting in their official capacities may be granted access to classified information upon presentation of proper credentials. In case of doubt about identity or the level of access authorized, DFS will verify these credentials or the level of access by contacting a security official of the agency or activity involved. (d)

Visits by Others (D)(continued)

Members of Congress and Congressional Staff (4)

Visits to NRC, NRC contractors, or other activities associated with the NRC program involving access to Restricted Data or other classified information by members of Congress or their staff may be approved by directors of headquarters offices or divisions, or by regional administrators. The identity of the visitors and their need-to-know must be established by the responsible congressional official or staff member. The proposed visit must be coordinated with the Director, DFS, to certify access authorization and with the Director, NRC Office of Congressional Affairs.

Immigrant Aliens Admitted to the United States for Permanent Residence (5)

Visit requests for immigrant aliens who possess DOD or NASA access authorization will be handled in accordance with the procedures specified in Section (D)(1) of this part. Procedures specified in Section (D)(2) of this part apply to those immigrant aliens who possess DOE access authorization. The procedures specified in Section (D)(3) of **this** part apply to those immigrant aliens who possess access authorization granted by Government agencies other than the DOD, NASA, and DOE.

Visits Involving Access to Sensitive Compartmented Information (SCI) (E)

Visitors to the NRC must have their SCI access authorization and need-to-know forwarded to the Special Security Officer in the ***NRC*** Division of Facilities and Security through SCI channels. **As** a minimum, the information required for these visits should include the full name of the visitor, the agency affiliation, the purpose of the visit, the date of the visit, the name of the person to be visited, and the SCI compartments involved. This information may be provided by telephone by a known or verifiable special security officer of the agency or department requesting the visit, by memorandum or teletype. If access to classified information other than SCI is involved, the need for **this** access must be certified and the required access authorization must be verified. (1)

Visits Involving Access to Sensitive Compartmented Information (SCI) (E) (continued)

NRC employees visiting other Government agencies or departments, or their contractors, shall contact the Special Security Officer in DFS to have their SCI access authorization properly forwarded to the agency to be visited. A request for access to classified information other than SCI may be included with the request for SCI or may be processed separately in accordance with the procedure specified in this part. (2)

Visits by Foreign Nationals Sponsored by Foreign Governments or International Organizations (F)

Requests for foreign nationals to visit NRC, NRC contractors, or other activities associated with the NRC program must be forwarded to the Director, DFS. Any security assurance the foreign nationals may possess must be officially certified to DFS by an authorized official of the foreign government sponsoring the visit, with the assistance of the Office of International Programs (OIP), if necessary. If the foreign nationals do not possess security assurance, OIP shall request DFS to conduct investigative checks. For further guidance on the disclosure of classified information to foreign nationals, refer to MD 12.2. **(1)**

Representatives of the International Atomic Energy Agency (IAEA) who are authorized to make visits to or inspect NRC-licensed facilities in accordance with the U.S./IAEA Safeguards Agreement may be authorized access to classified information, except for Restricted Data, on the basis of a DFS-issued disclosure authorization letter (DAL). The DAL will specify the names of the IAEA representatives and the classified information authorized, in addition to other relevant information. For further guidance on the disclosure of classified information to IAEA representatives, refer to MD 12.2. (2)

Visits to Foreign Governments or Activities by NRC Personnel *(G)*

For visits to foreign governments or activities by ***NRC*** personnel, an NRC Form277 should be submitted to DFS for processing and coordination with OIP when classified information is involved. If an NRC Form277 is not available, the information listed under Section (B)(12) of this part should be submitted to DFS. (1)

Visits to Foreign Governments or Activities by NRC Personnel *(G)* (continued)

These visit requests should be submitted at leas **30** days in advance of the initial visit date. (2)

Records of Visit Requests (H)

Records **of** visit requests consisting **of** the NRC Form277 or its equivalent and any related correspondence must be retained for 2 years after the expiration date of the visit authorized by the requesting office and the office of the facility visited.

Part III

Assignment of Foreign Regulatory Employees to NRC

Introduction (A)

Guidelines are given for the prevention of unauthorized access to classified information or sensitive unclassified information by foreign regulatory employees assigned to the NRC. The responsibilities of the Office of International Programs (OIP), the Division of Facilities and Security (DFS, Office of Administration), supervisors, and employees also are specified in this part.

Activity Plans (B)

OIP, in cooperation with DFS, will establish and coordinate the assignee program and individual assignee activity plans that enumerate the variety of activities in which the assignee is expected to participate.

Assignments *(C)*

Consideration for assignments will be given in the following order of priority: **(1)**

- Nationals from developing countries building or operating U.S.-type light water reactors (a)
- Nationals from other countries with which ***NRC*** has entered into information exchange and cooperation arrangements (b)
- Nationals from the International Atomic Energy Agency (IAEA) member states sponsored under the IAEA Fellowship Program, if different from Sections (C)(1)(a) and (b) of this part (c)
- Other foreign nationals as decided on a case-by-case basis (d)

Assignments (C) (continued)

Within each of these categories, preference will be given, in general, to nationals from countries party to the Treaty on the Non-Proliferation of Nuclear Weapons. Foreign nationals actively engaged in unsafeguarded nuclear activities in non-nuclear weapons states will not normally be selected. **(2)**

All personnel accepted for NRC assignments of generally not less than *6* months should—(3)

- Be fluent in English (a)
- Have successfully completed an NRC-approved English language foreign competency examination (b)
- Have professional training, experience, or education (c)
- Be certified as regular employees of either their national regulatory agencies or of other institutes or organizations responsible for performing domestic regulatory and safety functions (d)

The sponsoring government, institute, or other organization must bear all costs associated with the assignment, including, but not limited to, the assignee's salary, travel, and per diem. Any questions about costs should be referred to **OIP.** Assignees should be largely self-sufficient after orientation in order to minimize the impact on the NRC staff. Personal services such as assistance with housing and other orientation briefings will be handled by the Embassy of the assignee's country or by local representatives of his or her institution. Assignees will normally be given duties similar to those of NRC employees, without special "diverse experience" assignments, except when convenient to **NRC. (4)**

OIP must notify the Commission promptly whenever an application from a sensitive country is received to allow the Commission the opportunity to request any action they believe necessary while the staff is attempting to arrange placement and before any commitment is made. Another notification to the Commission must be prepared as soon as details of the proposed assignment are confirmed within the staff and at least 1 full week before the assignment **is** formally approved. Special care must be taken in regard to security considerations in selecting and screening foreign nationals, placing them within the staff, monitoring them closely, and educating their supervisors and co-workers. *(5)*

Assignments *(C)* (continued)

OIP shall forward all formal ***NRC*** letters of invitation accepting proposed assignments through State Department channels in conformance with and in furtherance of **U.S.** laws, regulations, and policy directives and objectives. Letters of invitation must be countersigned and returned to OIP 4 weeks before the assignee's expected arrival at the ***NRC. (6)***

OIP approves or disapproves the assignment of a foreign national to the ***NRC*** and designates the office to which the foreign national will be assigned, subject to the concurrence of the cognizant office director or regional administrator and DFS. (7)

Foreign nationals will not be assigned to the Commission, to the Office of the Secretary, to the Office of the Executive Director for Operations, to office directors, or to offices in which classified information or other sensitive information is often in use. Generally, assignments will not be made to branches in which large amounts of classified or other sensitive unclassified information is processed or stored, or to areas near these branches. (8)

Background Check (D)

Before inviting the foreign regulatory employee to join the ***NRC,*** OIP will obtain the required background and biographical data and submit it to DFS with a request that the appropriate indices check be conducted by the appropriate agencies (the Central Intelligence Agency, the Federal Bureau of Investigation, and the Department of State). Information that creates a question as to whether assignment of the foreign national is consistent with the national interest will be evaluated by DFS and forwarded with a recommendation to OIP.

Assignee Agreements (E)

Foreign assignees will be required to sign a commitment patterned after the agreement signed by the Government contract consultants agreeing not to take any proprietary documents away from their proper place of use and storage and not to disclose proprietary information or otherwise violate the conditions under which ***NRC*** staff members receive and use this information. The signing of the confidentiality agreement by the assignee is made a condition of the assignment under the terms of the agency-to-agency agreement that both the ***NRC*** and the foreign regulatory agency sign. Specific procedures are as follows:

Assignee Agreements (E)(continued)

- The supervisor of an assignee will make a determination of the need for an assignee to have access to proprietary information. **A** separate determination of need will be made for the proprietary information related to each program area in which the assignee is authorized to work. The supervisor will prepare a note concerning this access and will maintain a listing of documents to which the assignee has access. Whenever work on a program area is terminated, and at the end of each assignment, the assignee will return all proprietary documents. The supervisor of the assignee shall ensure that all documents on the assignee's list are returned. **(1)**

- Access to special classes of information identified in 10 CFR 2.790(d), including details of facility security plans, material control and accounting information, and Safeguards Information that is subject to 10 CFR 73.21, must not be granted **unless** approved by the Office of Nuclear Material Safety and Safeguards, Division of Fuel Cycle Safety and Safeguards **(NMSS/FCSS),** or the Office of Nuclear Reactor Regulation, Safeguards Branch **(NRR/PSGB),** in the case of reactors. (2)

Security Plans (F)

Representatives from DFS, OIP, and the office to which the foreign employee will be assigned will work together to define the assignment and to develop a security plan for each assignee. This task will be completed before the invitation letter is issued. The host office will be primarily responsible for developing the plan. This plan must be developed and approved before the assignee arrives. Each foreign assignee will be required to read, agree to, and sign the security plan. The plan will require the approval of OIP, the host office, and DFS and must include the following elements: **(1)**

- Description of the physical location of the assignment within NRC, a licensee facility, or another facility **(a)**

- Identification of specific areas to which assignees are to be given unescorted access in order to perform essential responsibilities (The assignee's access should be consistent with the requirements of DFS and the assignments of the host office.) (b)

- Explanation of special badging required and associated restrictions (c)

Security Plans (F) (continued)

- Explanation of restrictions on the use of, or connection to, NRC computing resources such as local area networks, other NRC computing systems, document management systems, and sensitive data. (d)
- Discussion of the ways in which commercial or foreign proprietary information must be protected if the assignment requires access to this information (Assignments should normally be tailored so that they do not require access to this information.) (e)
- Instructions on alerting co-workers about an assignee's presence and the assignee's restricted access, both physical and informational, including a DFS counterintelligence-type briefing ***(f)***
- Assignment of a supervisor and an alternate to monitor the assignee's day-to-day activities (g)
- Requirement for monthly or quarterly progress reports from the assignee (Copies of the report are to be sent to the supervisor and other appropriate persons in the office to which the foreign national is assigned.) (h)
- Requirement for a mid-point (or more frequent) interview by DFS of the assignee, the assignee's supervisors and, as appropriate, the assignee's co-workers to ensure that the assignee and supervisors are continuing to comply with the approved security plan (Any problems will be reported to OIP and any other appropriate office.) (i)

If later experience indicates that the security plan requirements cannot be met, or conditions change that warrant a possible change in requirements, or if any other problems arise, the supervisor will immediately advise OIP and DFS. Any changes in the security plan must be approved by DFS and **OIP.(2)**

DFS will issue assignees special identification badges. These badges, while allowing assignees unescorted access to specific areas, are prominently marked "Assignee" and are color-coded red for "no access." Foreign assignees will be required to wear their badges at all times. **(3)**

Security Plans (F)(continued)

Co-workers and other staff members in the assignee's area also will be made aware of the requirement for the assignee to wear his or her badge at all times. Access by the assignee into other areas not specified in the plan will require that the assignee be escorted by a cleared NRC employee designated by the assignee's supervisor. **(4)**

The assignee's supervisor will make an initial evaluation of an assignee's work area, as well as a reevaluation at the midpoint of the assignment and at any time the security plan is amended. Any recommendations should be given to DFS for action at this time. **(5)**

Assignee Responsibilities *(G)*

Assignees will not authorize visits by other individuals to NRC, NRC contractors, or other NRC facilities. **(1)**

Assignee duties are to be limited to those that do not require representing NRC in public or acting as an official representative in meetings with NRC licensees. ***(2)***

Assignees will be responsible for obtaining and making whatever copies of records or documents they desire to take with them before completion **of** their assignments. Assignees will be required to obtain the supervisor's approval before copying these records and will also be required to provide a list of these records to their ***NRC*** supervisors, OIP, and **DFS. (3)**

Evaluation of Assignees (H)

Upon completion of the assignment, OIP will provide an evaluation form to the supervisor. The supervisor shall complete the form and send copies of it to **OIP,** DFS, and the cognizant office director or regional administrator.

Exhibit 1

Due Process Procedures

Purpose of the Procedures (A)

The procedures specified herein are established for the conduct of hearings to determine the eligibility of NRC contractor personnel for unescorted access to nuclear power facilities, access to unclassified Safeguards Information (SGI), and access to sensitive NRC information technology systems and data under the NRC computer personnel screening program. Guidance is provided in 10 CFR **10.10** and 10.11 as to the types of information that raise questions concerning the consistency of an individual's eligibility for unescorted access to nuclear power facilities or access to unclassified **SGI** and the public health and safety; or for access to sensitive NRC information technology systems and data and the loss or harm that could result from improper operation of the information systems and from inadvertent or deliberate disclosure, alteration, or destruction of the data.

Notification to Individual of Hearing (B)

A notification letter providing the date, hour, and place of the hearing and the identity of the hearing official will be presented to each individual who has requested a hearing. When practicable, this letter will be presented to the individual in person at least **10** days in advance of the hearing, which will be scheduled with due regard for the convenience and necessity of the parties. The letter will be accompanied by a copy of these procedures and other administrative instructions, as necessary. **(1)**

The individual will have the right to appear personally before the hearing official and present evidence on his or her behalf through witnesses or by document or both, and may call, examine, and cross-examine witnesses. The individual may be present during the hearing to the extent permitted **by** national security concerns. The individual may be accompanied, represented, and advised by counsel or other representatives of his or her own choosing. In this case, the individual shall file with the Deputy Executive Director for Management Services (DEDM) a document designating the attorney or representative and authorizing him **or** her to receive all correspondence pertaining to the hearing. **(2)**

NRC Hearing Counsel (C)

The NRC hearing counsel assigned shall, before the scheduling of the hearing, review the information in the case and shall request the presence of witnesses and the production of documents and other physical evidence that the Division of Facilities and Security (DFS), Office of Administration (ADM), relied on to determine a substantial doubt exists concerning the individual's eligibility for unescorted access to nuclear power facilities, access to unclassified **SGI,** or access to sensitive NRC information technology systems and data.

Exhibit 1 (continued)

NRC Hearing Counsel *(C)* (continued)

When the presence of a witness and the production of documents and other physical evidence are deemed by the hearing counsel to be necessary or desirable for a determination of the issues, the Director, DFS shall make arrangements for the production of this evidence and for the witnesses to appear at the hearing by subpoena or by other means. **(1)**

The hearing counsel is authorized to communicate directly with the individual's counsel or representative, or the individual if the individual is not ***so*** represented, for purposes of mutually agreeing upon arrangements for expeditious hearing of the case. (2)

The individual is responsible for producing witnesses in his or her own behalf and presenting other evidence before the hearing official to support his or her position. The hearing counsel may at his or her discretion request the Director, DFS, to arrange for the issuance of subpoenas for witnesses to attend the hearing in the individual's behalf or for the production of specific documents or other physical evidence, provided the necessity for this assistance has been shown. **(3)**

Appointment of Hearing Official (D)

The ***NRC*** shall appoint a hearing official from a list of qualified attorneys possessing the highest degree of integrity, ability, and good judgment. To qualify, an attorney must have an ***NRC*"Q"** access authorization. No hearing official will be selected who has knowledge of the case or of any information relevant to the disposition of the case, or who for any reason would be unable to issue a fair and unbiased recommendation.

Prehearing Proceedings (E)

Before the hearing, the hearing official will be furnished the record in the case, consisting of the statement of charges and any associated amendment(s), the request for the hearing and the notice of hearing if it has been issued, and any agreements between the individual and the hearing counsel. **(1)**

The parties will be notified by the hearing official at least **10** days in advance of the hearing of the date, hour, and place of the hearing. The hearing official may order postponements or continuances from time to time for good cause shown. If, after due notice, the individual fails to appear at the hearing, or appears but is not prepared to proceed, the hearing official shall, unless good cause is shown, return the case to the DEDM who shall make the final determination on the basis of the information in the **NRC's** possession. (2)

Conduct of Hearing (F)

The hearing official shall conduct the hearing in an orderly, impartial, and decorous manner. Technical rules of evidence may be relaxed ***so*** that a full evidentiary record may be made based on all material and relevant facts. **(1)**

Exhibit 1 (continued)

Conduct of Hearing (F) (continued)

The proceedings will be open only to duly authorized NRC staff representatives, the individual, his or her counsel or representative, and those persons as may be officially authorized by the hearing official. Witnesses shall not testify in the presence of other witnesses except that the hearing official may, at his or her discretion, allow for expert witnesses to be present during testimony relevant to their own testimony. (2)

Witnesses, including the individual, shall be examined under oath or affirmation by the party who called them and may be cross–examined by the other party. The hearing official will rule on all evidentiary matters, may further examine any witness, and may call for additional witnesses or the production of documentary or other physical evidence if, in the exercise of his or her discretion, this additional evidence is deemed necessary to the resolution of an issue. **(3)**

If it appears during the hearing that Restricted Data or National Security Information may be disclosed, the hearing official shall ensure that disclosure is made only to persons authorized to receive it. **(4)**

The hearing official may permit the hearing counsel to amend the statement of charges to add or modify charges to be considered at any time during the hearing. In the event of such an amendment, the individual shall be given an opportunity to answer the amended charges. If the changes are of such a substantial nature that the individual cannot answer the amended charges without additional time, the hearing official shall grant such additional time as he or she deems necessary. ***(5)***

The hearing official may receive and consider evidence in the form of depositions or responses to interrogatories upon a showing that the witness is not available for good reason, such as death, serious illness, or similar cause, or in the form of depositions, interrogatories, affidavits, or statements with agreement of the parties. The hearing official may take official notice at any stage of the proceeding, where appropriate, of any fact not subject to reasonable dispute in that it is either generally known within the United States or capable of accurate and ready determination by resorting to sources whose accuracy cannot reasonably be questioned. A party is entitled, upon timely request, to an opportunity to be heard as to the propriety of taking such official notice. In the absence of prior notification, the request may be made after notice is taken. **(6)**

Records provided by investigative agencies that were compiled as a regular or routine procedure by the business or agency from which obtained, or other physical evidence other than investigative reports, may be received and considered subject to rebuttal without authenticating witnesses, provided that the investigative agency furnished this information to the **NRC** pursuant to its responsibilities in connection with assisting the NRC in determining the individual's eligibility. **(7)**

Records compiled in the regular course of business, or other physical evidence other than investigative reports, relating to a controverted issue that may not be inspected by the individual because they are classified may be received and considered, provided—(8)

Exhibit 1 (continued)

Conduct of Hearing (F) (continued)

- The DEDM has made a determination that the records or other physical evidence appears to be material. (a)
- The DEDM has made a determination that failure to receive and consider the records or other physical evidence would, in view of the fact that access eligibility is being sought, be substantially harmful to the **NRC** programs. (b)
- To the extent that national security permits, a summary or description of the records or other physical evidence is made available to the individual. In every such case, information as to the authenticity and accuracy of the physical evidence furnished by the investigative agency must be considered. (c)

Whenever information is made part of the record under Section **(F)(7)** or (F)(8) of this exhibit, the record must contain certification evidencing that the required determinations have been made. (9)

If the hearing official determines that additional investigation of any material information is required, he or she shall request in writing that the Director, DFS, arrange for the investigation and shall specify those issues for which more evidence is requested and identify, when possible, any persons or sources that might provide the evidence sought. **(10)**

A written transcript of the entire proceeding shall be made by a person possessing appropriate ***NRC*** access authorization and, except for portions containing Restricted Data or National Security Information, or other lawfully withholdable information, a copy of this transcript will be furnished the individual without cost. **(11)**

Recommendation of the Hearing Official ***(G)***

The hearing official's findings and recommendation shall be on the basis of the entire record, consisting of the transcript of the hearing, the documentary and other evidence adduced therein, and the statement of charges and any associated amendment and answer. The hearing official also shall consider the circumstances of the receipt of evidence and the nature and sensitivity of the job the individual is performing or may be expected to perform. **(1)**

The hearing official shall make specific findings on each charge in the statement of charges, including the reasons for his or her findings, and shall make a recommendation as to the action that should be taken in the case. **(2)**

The hearing official's recommendation shall be predicated upon his or her findings. If, after considering all the factors, the hearing official is of the opinion that the individual has clearly demonstrated that approving him or her for unescorted access to nuclear power facilities or for

Exhibit 1 (continued)

Recommendation of the Hearing Official (G) (continued)

access to unclassified SGI does not constitute an unreasonable risk to the public health and safety; or approving him or her for access to sensitive ***NRC*** information technology systems and data does not constitute an unreasonable risk to the security of such systems and data, a favorable recommendation must be made; otherwise, an adverse recommendation must be made. **(3)**

The hearing official shall submit his or her findings and recommendation in a signed report with the record of the case to the DEDM as soon as possible. (4)

The hearing official shall not consider the possible impact of the loss of the individual's services upon the ***NRC*** program. (5)

New Evidence (H)

After the close **of** the hearing, in the event the individual discovers new evidence not previously available or known to him or her, the individual may petition the hearing official if the hearing official's recommendation has not yet been issued, or thereafter, the DEDM to reopen the record to receive that evidence. If the hearing official or the DEDM, respectively, deems it material and appropriate, the record may be reopened to accept the evidence either by stipulation, with the agreement of the hearing counsel, or in a reconvened hearing.

Actions by the DEDM on the Recommendations (I)

Upon receipt of the findings and recommendation from the hearing official, and the record, the DEDM at his or her discretion may return the record for further proceedings by the hearing official with respect to specific matters designated by the DEDM. **(1)**

If no further proceedings are necessary, upon receipt of the findings and the recommendation by the hearing official, the DEDM, on the basis of the record accompanied by all findings and recommendations, shall make a final determination on whether the individual is eligible for unescorted access to nuclear power facilities, for access to unclassified **SGI,** or for access to sensitive ***NRC*** information technology systems and data. (2)

In making his or her determination, the DEDM shall give due consideration to the favorable as well as the unfavorable information concerning the individual. **(3)**

In the event of an adverse determination, the DEDM shall promptly notify the individual of his or her final decision concerning the individual's eligibility and of his or her findings with respect to each charge contained in the statement of charges. (4)

In the event of a favorable determination, the DEDM shall promptly notify the individual. (5)

Exhibit 2

Format for a Request for a Preappointment Investigation Waiver

MEMORANDUM TO: _____, Director
Office of Human Resources

FROM: (Requesting Office Director or Regional Administrator)

SUBJECT: AUTHORITY TO APPROVE THE EMPLOYMENT OF *AN* INDIVIDUAL BEFORE COMPLETION OF THE REQUIRED INVESTIGATION *AND* REPORT WHEN ACCESS TO CLASSIFIED MATTER IS NOT INVOLVED

This relates to the authority vested in the Deputy Executive Director for Management Services (DEDM) for approving employment of an ***NRC*** applicant before the completion of the required investigation when access to classified matter will not initially be required.

I request DEDM approval to employ the following individual(s) before the completion of the security investigation and report required by Section 145b of the Atomic Energy Act of 1954, as amended. The individual(s) has/have been selected to fill the position(s) indicated. Favorable preemployment checks have been conducted.

(Name(s)) (Position(s))

(Provide adequate justification for each request. Justification should not be standardized and should detail why a serious delay or interference to an ***NRC*** operation or program will result if the request is not approved. Note: If the request involves interim unescorted access to nuclear power plants for inspectors and resident clerical aides or a recommendation for waiving personnel reference checks for NRC consultants or experts, it should be clearly stated in the justification.)

Administrative controls will be established to ensure that (the individual(s)) will not have access to National Security Information or Restricted Data until he/she/they is/are granted an access authorization by the Division of Facilities and Security, Office of Administration.

Exhibit 3

Preemployment Screening and Section 145b Processing Procedures for NRC Applicants

The headquarters Human Resources (HR) specialist or the Regional HR Officer will—(A)

- Obtain security forms from the selectee (1)
- Ensure that character and employment reference checks covering the required number of years are conducted in accordance with the standard operating procedures of Exhibit 4 to this handbook (2)
- Evaluate and certify the acceptability of the character and employment reference checks (3)

The required documentation for all acceptable packages (consisting of the Standard Form 86, Parts 1 and 2; two fingerprint charts; and *NRC* Form E—1,176 and 354) will be forwarded to the Division of Facilities and Security (DFS), Office of Administration. This documentation will include the memorandum requesting a preappointment waiver and certifying need by the regional administrator, the office director, or the deputy office director, pursuant to Section 145b of the Atomic Energy Act of 1954, as amended. **(B)**

Upon receipt of the Section 145b package, DFS will—(C)

- Request the Office of Personnel Management to conduct a National Crime Information Center (NCIC) check on the selectee (1)
- Conduct an online computer credit check of the selectee (2)
- **If** deemed necessary, telephonically conduct a security assurance interview with the selected applicant **to** discuss in detail the answers provided on the **SF** 86, as well as any other matters of security concern (3)
- Evaluate the eligibility of the applicant for a Section 145b ***employment waiver*** on the basis of a review of the final package and the results of the credit check, the NCIC check, and the security interview, if conducted, and recommend approval or disapproval (4)

Exhibit 4

Standard Operating Procedures for Preemployment Screening of NRC Applicants

The headquarters Human Resources (HR) specialist or the Regional HR Officer will obtain a current Optional Form (OF) 612, Standard Form (SF) 171, or equivalent and security forms package (consisting of the SF 86, Parts 1 and 2; two fingerprint charts; and NRC Forms E–1, 176, and 354) from the selectee. The HR specialist or the Regional HR Officer will ensure that appropriate reference checks are conducted using the OF 612, **SF** 171, or equivalent and the SF 86, Part 1, as the source documents. **(A)**

The reference checks will generally follow the format of NRC Form 212, "Qualifications Investigation," plus additional requirements as indicated below. Questions 23, 24, 25, and 26 must be asked of each source. Space is provided on the form for annotations and appropriate comments. Additional pages should be used as needed. (B)

The following additional requirements apply: (C)

- All personnel conducting reference checks must be thoroughly familiar with the NRC Form 212 and reference check techniques. **(1)**
- Using the OF 612, SF171, or equivalent and the SF86, Part 1, as guides, identify employers for at least the past 5 years, where applicable. (2)
- On the basis of the answer to each item or question on NRC Form 212, ask as many followup questions as needed to develop a full response. (3)
- For applicants other than students being considered for temporary summer appointments, reference checks must cover at a minimum the last 5 years. For applicants who do not have 5 years of employment experience, obtain, if possible, references from high school or college sources, as appropriate, to cover at least the past 5 years. For students being considered for temporary summer employment, conduct supervisory reference checks for all jobs held during the past 2 years, where applicable. For students who do not have 2 years of employment experience, obtain, if possible, references from school and other sources. In either case, at least two references are required. If any adverse employment or security-related information is noted or developed during processing, the student will be processed in accordance with the normal processing procedures. Summer employees other than students are subject to the normal processing procedures. **(4)**
- In all cases, verify dates of attendance at the educational institution, the highest educational level attained, and the type and year of degree. (5)

Exhibit 4 (continued)

Standard Operating Procedures for Preemployment Screening of NRC Applicants (continued)

- To supplement the education and employment history for applicants other than students being considered for summer employment, develop at least one additional source on the applicant (developed references are not required for students being considered for summer employment). This additional source must not be an individual listed on the OF 612, **SF** 171, or equivalent or the **SF** 86 or otherwise provided by the applicant. This source may be developed by asking employers or those responding to education questions if they can name anyone else who has personal knowledge of the applicant. Use ***NRC*** Form 212 to obtain the reference from the developed source. (6)

The HR specialist or the Regional HR Officer will review the results of all the reference checks to determine acceptability of the applicant. If either the HR specialist or the Regional HR Officer has any doubt as to the applicant's acceptability, he or she must discuss whether to proceed with the selecting official. If the decision is to proceed with the applicant, the HR specialist or the Regional HR Officer will certify the acceptability of the Section 145b package and will send the complete security forms package, the Section 145b request memorandum, all reference checks, and any other documentation normally required to DFS by overnight mail if from a region or by interoffice mail if from a headquarters office. (D)

Exhibit 5

Expedited Temporary Unescorted Access Approval for NRC Employees, Including Inspectors and Resident Clerical Aides

The preemployment screening and processing procedures to meet Section 145b requirements for NRC applicants (Exhibit **3** of this handbook) will proceed as usual. The following steps, as applicable, are to be followed when temporary unescorted access is required:

The Regional Human Resources (HR) Officer will initiate processing of security forms from the selectee. The Regional HR Officer will immediately forward to Division of Facilities and Security (DFS), by overnight mail, an advance copy of Standard Form (SF) 86, "Questionnaire for National Security Positions," two fingerprint cards, and a copy of the Optional Form (OF) 612, SF 171, or equivalent completed by the individual. (1)

- Upon receipt of these forms, DFS will conduct a National Crime Information Center (NCIC) check and the required online credit checks. The credit and NCIC checks must be completed before unescorted access is granted. **(2)**

Upon the Regional HR Officer's completion and evaluation of character and employment reference checks on the selectee, the Regional HR Officer will forward the results of these checks to HR via overnight mail. If the Regional HR Officer has been delegated the authority to submit the documentation directly to DFS by the Director, HR, the Regional HR Officer may make and certify the acceptability of reference checks in accordance with paragraph (5) of this exhibit. The original security forms on the selected applicant, the memorandum requesting a preappointment waiver and certifying need for immediate employment by the regional administrator or the deputy pursuant to Section 145b, and all other documentation normally required also will be forwarded if it has not already been submitted. **(3)**

- The regional administrator will document the need for an additional security interview by DFS for ***temporary unescorted access*** to the protected or vital areas of a nuclear power plant, pending the grant of an **NRC** security clearance. (4)
- HR will evaluate the acceptability of character and employment reference checks and will forward the acceptable packages to DFS. (5)
- Upon receipt of the final acceptable package from HR, DFS will conduct a security assurance interview by telephone with the selected applicant to discuss in detail the answers provided on the SF 86, as well as any other matters of security concern. DFS will then evaluate the applicant based on a review of the final package and the results of the credit check, the NCIC check, and the security interview. DFS will advise the regional administrator of its "no objection" or "objection" to the approval of temporary

Exhibit 5 (continued)

Expedited Temporary Unescorted Access Approval for NRC Employees, Including Inspectors and Resident Clerical Aides (continued)

unescorted access, pending the grant of the security clearance. **DFS** must be provided with a copy **of** the regional administrator's final decision. **(6)**

- **DFS** will advise the regional office and **HR** when **DFS** receives any significant adverse information on an individual who is on board or being processed that raises immediate security concerns. **DFS** will recommend to the regional administrator whether temporary unescorted access approval, if access has been granted, should be rescinded pending the resolution of security concerns under the provisions **of** 10 **CFR** Part 10. The regional administrator will decide whether temporary unescorted access approval should be rescinded and shall notify **DFS** of the decision. **(7)**

Exhibit 6
"Q" and "L" Reinvestigation Program Requirements

“Q” and Sensitive Compartmented Information (SCI) Reinvestigation Requirements (I)

For employees, consultants experts, panel members, former senior NRC officials, contractors and agents of the NRC, and congressional staff members-

0 Each individual to be reinvestigated shall submit a new Questionnaire for National Security Positions (QSP, Standard Form 86) and related forms, including an NRC Form 176, “Security Acknowledgment.” These forms will be the basis for an investigation as specified below. (1)

0 ***An*** OPM single-scope background investigation periodic reinvestigation **(SSBI--PR)** will be conducted for “Q” and SCI cleared individuals other than the Chairman, Commissioners, and the Inspector General who are subject to an FBI (re)investigation in connection with their presidential appointment. (2)

0 Further investigative coverage may be undertaken on a case-by-case basis if the scheduled coverage is insufficient to obtain the required information. **(3)**

"L" Reinvestigation Program Requirements (II)

Each individual to be investigated shall submit a new QSP and related forms, including an NRC Form 176, “Security Acknowledgment.” These forms will be the basis for an investigation as follows:

0 A national agency check with law and credit (NACLC) shall be conducted. The investigation may be expanded as necessary to determine if access is clearly consistent with national security. (1)

0 Further investigative coverage may be undertaken on a case-by-case basis if the scheduled coverage is insufficient to obtain the required information (2)

0 Although not normally required for “Q” or **"L"** reinvestigations, a new set of fingerprint cards may be requested on a case-by-case basis. **(3)**

Exhibit 7
Procedures for the Conduct of Hearings Under 5 U.S.C. 7532

Purpose of the Procedures (A)

The procedures set forth below are established for the conduct of hearings pursuant to 5 U.S.C. 7532 to determine whether an individual's continued employment with the ***NRC*** is clearly consistent with the national security. Guidance is provided in 10 CFR 10.10 and 10.11 as to the types of information that raise questions concerning the consistency of an individual's employment and the national security.

Notification to Individual of Hearing (B)

A notification letter providing the date, hour, and place of the hearing and the identity of the hearing official will be presented to each individual who has requested a hearing. Where practicable, this letter will be presented to the individual in person at least 10 days in advance of the hearing, which will be scheduled with due regard for the convenience and necessity of the parties. The letter will be accompanied by a copy of these procedures and other administrative instructions, as necessary. **(1)**

The individual will have the right to appear personally before the hearing official and present evidence in his or her behalf through witnesses or by document or both, and may call, examine, and cross-examine witnesses. The individual may be present during the hearing to the extent permitted by national security concerns. The individual may be accompanied, represented, and advised by counsel or other representatives of his or her own choosing. In this case, the individual shall file with the Deputy Executive Director for Management Services (DEDM) a document designating the attorney or representative and authorizing him or her to receive all correspondence pertaining to the hearing. (2)

NRC Hearing Counsel *(C)*

The ***NRC*** hearing counsel assigned shall, before the scheduling of the hearing, review the information in the case and shall request the presence of witnesses and the production of documents and other physical evidence relied upon in suspending the individual pursuant to the provisions of 5 U.S.C. 7532. When the presence of a witness and the production of documents and other physical evidence are deemed by the hearing counsel to be necessary or desirable for a determination of the issues, the Director, Division of Facilities and Security **(DFS),** Office of Administration, shall make arrangements for the production of this evidence and for the witnesses to appear at the hearing by subpoena or by other means. **(1)**

The hearing counsel is authorized to communicate directly with the individual's counsel or representative, or the individual if the individual is not so represented, for purposes of mutually agreeing upon arrangements for expeditious hearing of the case. (2)

Exhibit 7 (continued)

Procedures for the Conduct of Hearings Under 5 U.S.C. 7532 (continued)

NRC Hearing Counsel (C) (continued)

The individual is responsible for producing witnesses in his or her own behalf and presenting other evidence before the hearing official to support his or her position. The hearing counsel may at his or her discretion request the Director, DFS, to arrange for the issuance of subpoenas for witnesses to attend the hearing in the individual's behalf or for the production of specific documents or other physical evidence, provided the necessity for this assistance has been shown. **(3)**

Appointment of Hearing Official (D)

The NRC shall appoint a hearing official from a list of qualified attorneys possessing the highest degree of integrity, ability, and good judgment. To qualify, an attorney must have an ***NRC* "Q"** access authorization. No hearing official will be selected who has knowledge of the case or of any information relevant to the disposition of the case, or who for any reason would be unable to issue **a** fair and unbiased recommendation.

Prehearing Proceedings (E)

Before the hearing, the hearing official will be furnished the record in the case, consisting of the statement of charges and any associated amendment(s), the request for the hearing and the notice of hearing if it has been issued, and any agreements between the individual and the hearing counsel. **(1)**

The parties will be notified by the hearing official at least 10 days in advance of the hearing of the date, hour, and place of the hearing. The hearing official may order postponements or continuances from time to time for good cause shown. If, after due notice, the individual fails to appear at the hearing, or appears but is not prepared to proceed, the hearing official shall, unless good cause is shown, return the case to the DEDM who shall make the final determination on the basis of the information in the **NRC's** possession. **(2)**

Conduct of Hearing (F)

The hearing official shall conduct the hearing in an orderly, impartial, and decorous manner. Technical rules of evidence may be relaxed so that a full evidentiary record may be made based on all material and relevant facts. **(1)**

Exhibit 7 (continued)

Procedures for the Conduct of Hearings Under 5 U.S.C. 7532 (continued)

Conduct **of Hearing** (F) (continued)

The proceedings will be open only to duly authorized NRC staff representatives, the individual, his or her counsel or representative, and those persons as may be officially authorized by the hearing official. Witnesses shall not testify in the presence of other witnesses except that the hearing official may, at his or her discretion, allow for expert witnesses to be present during testimony relevant to their own testimony. (2)

Witnesses, including the individual, shall be examined under oath or affirmation by the party who called them and may be cross-examined by the other party. The hearing official will rule on all evidentiary matters, may further examine any witness, and may call for additional witnesses or the production of documentary or other physical evidence if, in the exercise of his or her discretion, this additional evidence is deemed necessary to the resolution **of** an issue. **(3)**

If it appears during the hearing that Restricted Data or National Security Information may be disclosed, the hearing official shall ensure that disclosure is made only to persons authorized to receive it. **(4)**

The hearing official may permit the hearing counsel to amend the statement of charges to add or modify charges to be considered at any time during the hearing. In the event of such an amendment, the individual shall be given an opportunity to answer the amended charges. If the changes are of such a substantial nature that the individual cannot answer the amended charges without additional time, the hearing official shall grant such additional time as he or she deems necessary. (5)

The hearing official may receive and consider evidence in the form of depositions or responses to interrogatories upon a showing that the witness is not available for good reason, such as death, serious illness, or similar cause, or in the form of deposition, interrogatories, affidavits, or statements with agreement of the parties. The hearing official may take official notice at any stage of the proceeding, where appropriate, of any fact not subject to reasonable dispute in that it is either generally known within the United States or capable of accurate and ready determination by resorting to sources whose accuracy cannot reasonably be questioned. A party is entitled, upon timely request, to an opportunity to be heard as to the propriety of taking such official notice. In the absence of prior notification, the request may be made after notice is taken. **(6)**

Exhibit 7 (continued)

Procedures for the Conduct of Hearings Under 5 U.S.C. 7532 (continued)

Conduct of Hearing (F) (continued)

Records provided by investigative agencies that were compiled as a regular or routine procedure by the business or agency from which obtained, or other physical evidence other than investigative reports, may be received and considered subject to rebuttal without authenticating witnesses, provided that the investigative agency furnished this information to the ***NRC*** pursuant to its responsibilities in connection with assisting the NRC in determining the individual's eligibility for reinstatement consistent with the national security. **(7)**

Records compiled in the regular course of business, or other physical evidence other than investigative reports, relating to a controverted issue that, because they are classified, may not be inspected by the individual, may be received and considered, provided—(8)

- The DEDM has made a determination that the records or other physical evidence appears to be material. (a)
- The DEDM has made a determination that failure to receive and consider the records or other physical evidence would, in view of the fact that access authorization and/or employment clearance is being sought, be substantially harmful to the national security. (b)
- To the extent that national security permits, a summary or description of the records or other physical evidence is made available to the individual. In every such case, information as to the authenticity and accuracy of the physical evidence furnished by the investigative agency must be considered. (c)

Whenever information is made part of the record under Section **(F)(7)** or (8) of **this** exhibit, the record must contain certification evidencing that the required determinations have been made. **(9)**

If the hearing official determines that additional investigation of any material information is required, he or she shall request in writing that the Director, DFS, arrange for the investigation and shall specify those issues upon which more evidence is requested and identify, where possible, any persons or sources that might provide the evidence sought. (10)

A written transcript of the entire proceeding shall be made by a person possessing appropriate NRC access authorization and/or employment clearance and, except for portions containing Restricted Data or National Security Information, or other lawfully withholdable information, a copy of this transcript shall be furnished the individual without cost. **(11)**

Exhibit 7 (continued)

Procedures for the Conduct of Hearings Under 5 U.S.C. 7532 (continued)

Recommendation of the Hearing Official (G)

The hearing official's findings and recommendation shall be based upon the entire record consisting of the transcript of the hearing, the documentary and other evidence adduced therein, and the statement of charges and any associated amendment and answer. The hearing official also shall consider the circumstances of the receipt of evidence and the nature and sensitivity of the job the individual was performing. **(1)**

The hearing official shall make specific findings on each charge in the statement of charges, including the reasons for his or her findings, and shall make a recommendation as to the action that should be taken in the case. (2)

The hearing official's recommendation shall be predicated upon his or her findings. If, after considering all the factors, the hearing official is of the opinion that the individual has clearly demonstrated that reinstating his or her access authorization and/or employment clearance, or reinstatement **of** employment will not endanger the national security, a favorable recommendation must be made; otherwise, an adverse recommendation must be made. **(3)**

The hearing official shall submit his or her findings and recommendation in a signed report with the record of the case to the DEDM as soon as possible. **(4)**

The hearing official shall not consider the possible impact of the loss of the individual's services upon the ***NRC*** program. ***(5)***

New Evidence (H)

After the close of the hearing, in the event the individual discovers new evidence not previously available or known to him or her, the individual may petition the hearing official if the hearing official's recommendation has not yet been issued, or thereafter, the DEDM to reopen the record to receive that evidence. If the hearing official or the DEDM, respectively, deems it material and appropriate, the record may be reopened to accept the evidence either by stipulation, with the agreement of the hearing counsel, or in a reconvened hearing.

Exhibit 7 (continued)

Procedures for the Conduct of Hearings Under 5 U.S.C. 7532 (continued)

Actions by the DEDM on the Recommendations (I)

Upon receipt of the findings and recommendation from the hearing official, and the record, the DEDM at **his** or her discretion may return the record for further proceedings by the hearing official with respect to specific matters designated by the DEDM. **(1)**

If no further proceedings are necessary, upon receipt of the findings and the recommendation by the hearing official, the DEDM, on the basis of the record accompanied by all findings and recommendations, shall make a final determination whether the individual will be reinstated or removed in the interest of national security. ***(2)***

In making the determination as to whether the individual will be reinstated or removed in the interest of national security, the DEDM shall give due recognition to the favorable as well as the unfavorable information concerning the individual. **(3)**

In the event of an adverse determination, the DEDM shall promptly notify the individual of **his** or her final decision to remove that individual in the interest of national security and of **his** or her findings with respect to each charge contained in the statement of charges. **(4)**

In the event of a favorable determination, the DEDM shall promptly notify the individual. *(5)*

U.S. NUCLEAR REGULATORY COMMISSION

DIRECTIVE TRANSMITTAL

TN: DT–99–31

To: NRC Management Directives Custodians

Subject: Transmittal of Directive 12.4, "NRC Telecommunications Systems Security Program"

Purpose: Directive and Handbook 12.4 have been revised to reflect changes in organizational responsibilities and delegations of authority for the Chief Information Officer and the Division of Facilities and Security, Office of Administration (ADM). ADM will assume primary responsibility for NRC secure telecommunications programs, including planning, budgeting, and support. This change also removes two examples of protected telephone systems that are no longer valid.

Office and Division of Origin: Office of Administration

Contact: Nancy Fontaine, 301–415–1253

Date Approved: January 21,1998 (Revised: December 8, 1999)

Volume: 12 Security

Directive: 12.4 NRC Telecommunications Systems Security Program

Availability: Rules and Directives Branch
Office of Administration
David L. Meyer (301)415–7162 or
Jeannette P. Kiminas (301)415–7086

NRC Telecommunications Systems Security Program

Directive 12.4

Contents

Policy 1

Objectives 1

Organizational Responsibilities and Delegations of Authority 2

Deputy Executive Director for Management Services (DEDM) 2
Chief Information Officer (CIO) 2
Office Directors and Regional Administrators 3
Director. Division of Facilities and Security (DFS).
Office of Administration (ADM) 3
Director. Division of Contracts and Property Management (DCPM). ADM 5
Associate Director for Training and Development.
Office of Human Resources (HR) 5

Applicability 6

Handbook 6

References 6

NRC Telecommunications Systems Security Program Directive 12.4

Policy
(12.4–01)

It is the policy of the **U.S.** Nuclear Regulatory Commission that **all** classified or sensitive unclassified information transmitted on telecommunications systems that are under the security jurisdiction of the **NRC** be protected as required by law.

Objectives
(12.4–02)

- To safeguard the following information that is communicated on telecommunications systems. (021)
  - National Security Information (a)
  - Restricted Data and formerly Restricted Data (b)
  - Sensitive unclassified information (c)
    - Privacy information (i)
    - Proprietary Information (ii)
    - Safeguards Information (iii)
  - Other sensitive information as defined by the Computer Security Act of **1987 (d)**
- To safeguard classified or sensitive unclassified information communicated over telecommunications systems that prepare, transmit, communicate, or process the information (writing, images, sounds, or other data) by electrical, electromagnetic, electromechanical, electro-optical, or electronic means, using

Objectives

(12.4–02) (continued)

media such as twisted pair cable, coaxial cable, fiber optic cable, microwave, or satellite. These telecommunications systems include, but are not limited to, the following: (022)

- Telephones (a)
- Facsimiles (b)
- Radios (c)
- Video and video-teleconferencing systems **(d)**
- Networks (i.e., local area network and wide area network) (e)
- Other data transmission systems ***(f)***

Organizational Responsibilities and Delegations of Authority

(12.4-03)

Deputy Executive Director for Management Services (DEDM)

(031)

- Acts as the Senior Agency Official for issues involving classified information. (a)
- Authorizes, directly or by designee, exceptions to or deviations from this directive within the limitations of authority set by law and Federal regulation. (b)

Chief Information Officer (CIO)

(032)

- Reviews and approves, in conjunction with the Division of Facilities and Security (DFS), Office of Administration, security proposals and plans originated by **NRC** offices, licensees, certificate holders, and contractors, for telecommunications systems, facilities, and communication centers to be used for communicating classified or sensitive unclassified information. (a)

Chief Information Officer (CIO)

(032) (continued)

- Reviews and concurs in feasibility studies for requested new **NRC** telecommunications systems that will communicate classified or sensitive unclassified information. (b)
- Reviews information copies of facility security surveys conducted by **DFS** on non-network systems that handle classified or sensitive unclassified infomation; acts on specific recommendations in accordance with Handbook 12.4. (c)
- Provides engineering design services for all cryptographic and related terminal equipment that interfaces with common carrier circuitry; orders the installation of this equipment. (d)
- Reviews, comments, and concurs in documents of the National Security Telecommunications and Information Systems Security Committee (NSTISSC). (e)
- Appoints an observer to the Subcommittee on Information Systems Security. ***(f)***
- Provides technical support and installation of high-speed data lines, as needed. (g)

Office Directors and Regional Administrators

(033)

- Specify, budget, order, install, move, test, and maintain telecommunication systems under their jurisdiction and arranges for appropriate training **of** personnel. (a)
- Ensure that all secure telecommunications systems operated by NRC or NRC contractors comply with this directive and handbook to safeguard classified or sensitive unclassified information. (b)

Director, Division of Facilities and Security (DFS), Office of Administration (ADM)

(034)

- Ensures that classified or sensitive unclassified information processed by systems used by NRC headquarters and regional offices is safeguarded. (a)

Director, Division of Facilities and Security (DFS), Office of Administration (ADM)
(034) (continued)

- Reviews and approves NRC security proposals and plans, contracts, and interagency agreements involving classified or sensitive unclassified information; conducts feasibility studies and issues security requirements for systems that communicate classified or sensitive unclassified information. (b)
- Conducts system security surveys and provides followup recommendations to ensure compliance with security policies for non-network systems that handle classified or sensitive unclassified information. (c)
- Serves as the observer to NSTISSC and observer to the NSTISSC Subcommittee on Telecommunications Security. (d)
- Serves as the NRC representative to the National Security Agency for all matters relating to communications security (COMSEC), such as COMSEC accounting, COMSEC training, and the Central Office of Record. (e)
- Serves as the Command Authority for the secure telephone unit and secure terminal equipment; appoints user representatives for NRC and specifies key ordering privileges. ***(f)***
- Manages and operates the Secure Communications Center, including budgeting, ordering, installing, moving, testing, and maintaining telecommunications systems. (g)
- Specifies, budgets, orders, installs, moves, tests, and maintains agency infrastructure components, including NRC headquarters telecommunications systems that communicate classified or sensitive unclassified information; trains or arranges training for personnel on these systems; originates statements of work, work orders, and requests for procurement action. (h)
- Approves all purchase requests from NRC regions for telecommunications systems that transmit classified or sensitive unclassified information. (i)
- Coordinates services performed by the General Services Administration or other contractors, including issuing necessary budget documents and work orders for cryptographic, red/black wiring, and installation for telecommunications systems that process classified information. **(j)**

Director, Division of Facilities and Security (DFS), Office of Administration (ADM)

(034) (continued)

- Ensures, through proper coordination with the Personnel Security Branch, that all individuals designated to participate in the design, planning, operation, or maintenance of NRC telecommunications systems, or centers that communicate classified or sensitive unclassified information, are properly screened and eligible for access to this information or these systems before this access is granted. (k)
- Ensures the adequacy of the security requirements included in contracts, interagency agreements, and designs for NRC telecommunications systems that handle classified or sensitive unclassified information. (l)
- Determines requirements for cryptographic equipment and defines specifications for the acquisition and implementation of automated information equipment or systems that process or produce classified or sensitive unclassified information. (m)
- Ensures that any construction, expansion, or restack of NRC areas or facilities having or requiring telecommunications systems, is coordinated with Office of the CIO (OCIO) during both planning and installation phases. (n)

Director, Division of Contracts and Property Management (DCPM), ADM

(035)

- Ensures that all Federal and NRC requirements for the protection of classified or sensitive unclassified information are provided in solicitations and contracts. (a)
- Ensures that redistribution, destruction, and disposal of NRC telecommunications systems that have been used to process classified or sensitive unclassified information, is coordinated through OCIO and DFS before release. (b)

Associate Director for Training and Development, Office of Human Resources (HR)

(036)

- Assists in the development and delivery of appropriate security training programs for NRC personnel who work on NRC telecommunications systems, as requested. (a)

Associate Director for Training and Development, Office of Human Resources (HR)
(036) (continued)

- Provides other security-related training, as requested. (b)
- Ensures the inclusion of a security briefing in the initial orientation of new employees. (c)

Applicability
(12.4–04)

The policy and guidance in this directive and handbook apply to all NRC employees, consultants, experts, panel members, contractors, and subcontractors who transmit classified or sensitive unclassified information on telecommunications systems that are under the jurisdiction of NRC, including those performing work for the NRC pursuant to interagency agreements, memoranda of understanding, or financial assistance programs. This directive does not apply to NRC licensees or certificate holders.

Handbook
(12.4–05)

Procedures and guidelines for implementation of the telecommunications systems security program are contained in Handbook 12.4.

References
(12.4–06)

Computer Security Act of 1987, Pub. L. 100-235.

Management Directive 3.2, "Privacy Act."

— 12.1, "NRC Facility Security Program."

— 12.2, "NRC Classified Information Security Program."

— 12.3, "NRC Personnel Security Program."

— 12.5, "NRC Automated Information Systems Security Program."

— 12.6, "NRC Sensitive Unclassified Information Security Program."

References

(12.4–06) (continued)

National Security Agency (NSA),* Electronic Key Management System **(EKMS)** 702.01, "STU-III Key Management Plan," and supplements.

–, Manual 90-2, "COMSEC Material and Control Manual."

National Security Decision Directive 145, "National Policy on Telecommunications and Automated Information Systems Security."

National Security Telecommunications and Information Systems Security (NSTISSI),** No. **4001,** "Controlled Cryptographic Items."

–, No. 4005, "Safeguarding COMSEC Facilities and Material."

Office **of** Management and Budget Circular **A-130,** "Management of Federal Information Resources."

National Security Telecommunications and Information Systems Security Advisory Memorandum TEMPEST 2-95, "Guidelines for Facility Design and Red/Black Installation," dated November 1,1995.

* Copies of NSA documents are available to all ***NRC*** personnel assigned COMSEC responsibilities, or upon written request to the Director, DFS.

** Contact the Chief, INFOSEC, for a copy of NSTISSI documents.

NRC Telecommunications Systems Security Program

Handbook 12.4

Contents

Part I

Introduction 1

Part II

Security of Telecommunications 3

Communications Security (COMSEC) (A) 3
General (1) 3
Sensitivity of COMSEC Information (2) 3
COMSEC Material and Equipment (3) 3
Control of COMSEC Material (4) 4
Controlled Cryptographic Items (CCI) (5) 4
Other Materials (6) 4
Access to Cryptographic and COMSEC Information (7) 5
NRC Contractor COMSEC Authorizations (8) 6
COMSEC Functional Designations and Responsibilities (9) 6
Installation of COMSEC Equipment (10) 8
Acquisition of COMSEC Material (11) 8
Releasing COMSEC Information to U.S. Contractors and Other Sources Outside the U.S. Government (12) 9
Reporting COMSEC Insecurities (Incidents) (13) 9
COMSEC Emergency Procedures (14) 10
Secure Telecommunications Facilities Requirements (B) 11
Safeguarding COMSEC Facilities (1) 11
Establishment of a Secure Telecommunications Facility (2) 11
Security Clearance for Installation, Maintenance, and Modification (3) 12
Guidelines for Facility Design and Red/Black Installation (4) 13
Operation of Secure Telecommunications Facilities (C) 13
General Guidelines and Procedures (1) 13
Standard Operating Procedures (2) 13
Equipment Operation (3) 13
Handling of Information (4) 14
Security Surveys of Telecommunications Systems (5) 14
Followup of Deficiencies (6) 14

Contents (continued)

Part II (continued)

Transmission and Emission Security (D) 15
Transmission Security (1) 15
Emission Security (2) 15
TEMPEST(3) 16
Technical Security Inspections (4) 16
Protection of Sensitive Unclassified Information (E) 16
Telecommunications Protection Authority (1) 16
Telecommunications Protection Procedures (2) 17
Secure Telecommunications Systems at NRC (F) 18
General (1) 18
Security Proposals and Plans (2) 18
Review of Telecommunications Traffic (3) 18
Record Telecommunications (4) 19
Voice Telecommunications (5) 20

Exhibit

"Format and Guidelines for a Secure Telecommunications Facility Proposal or Plan" 25

Part I
Introduction

This handbook contains the procedures for planning, implementing, maintaining, and monitoring the security of NRC contractor and NRC telecommunications systems that communicate classified and sensitive unclassified information. It does not address traditional computer security or physical security issues except when they are directly related to the protection of information during processing or transmission. This handbook is intended for use in combination with other management directives and handbooks, and in conjunction with National Security Telecommunications and Information Systems Security (NSTISS) publications, National Security Agency (NSA) Communications Security (COMSEC) publications, and NRC policies. (A)

A list of the Federal authorities involved with telecommunications systems security is given below. (B)

- **National Security Council/Policy Coordinating Committee (NSC/PCC) for National Security Telecommunications and Information Systems (1)**

  This committee consists of the Secretary of State, the Secretary of the Treasury, the Attorney General, the Secretary of Energy, the Secretary of Commerce, the Director of Central Intelligence, the Assistant Director for National Security Affairs, the Director of the Office of Management and Budget, the Senior Director for Defense Policy and *Arms* Policy of the NSC, and **is** chaired by the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence). The National Manager for NSTISS participates as an observer.

- **The National Security Telecommunications and Information Systems Security Committee (NSTISSC) (2)**

  This committee is established to operate under the guidance of the NSC/PCC for National Security Telecommunications and

Information Systems to consider technical matters and develop operating policies, procedures, guidelines, instructions, and standards as necessary to implement the provisions of the directive entitled "National Policy for the Security of National Security Telecommunications and Information Systems." The NRC is a non-voting member of this committee.

- **Executive Agent of the Government for National Security Telecommunications and Information Systems Security (3)**

  The Secretary of Defense is the Executive Agent of the Government for NSTISS and is responsible for implementing, under his signature, the policies developed by the NSTISSC.

- **National Manager for National Security Telecommunications and Information Systems Security (4)**

  The Director, **NSA,** is designated the National Manager for NSTISS. The NSA prescribes or approves all cryptographic systems and techniques used by or on behalf of the **U.S.** Government. These responsibilities include, but are not limited to:

  - Conducting, approving, or endorsing research and development of techniques and equipment to secure national security systems (a)
  - Reviewing and approving all standards, techniques, systems, and equipment related to the security **of** national security systems (b)
  - Prescribing the minimum standards, methods, and procedures for protecting cryptographic and other technical security material, techniques, and information related to national security systems (c)

Part II
Security of Telecommunications

Communications Security (COMSEC) (A)

General (1)

Communications security is the protection of information while it is being transmitted by telephone, cable, microwave, satellite, or any other means. It includes cryptographic security, transmission security, emission security, and physical security of COMSEC material. COMSEC is a program that certifies cryptographic and other communications security products.

Sensitivity of COMSEC Information (2)

COMSEC information is considered especially sensitive because of the need to safeguard **U.S.** cryptographic principles, methods, and material against exploitation.

COMSEC Material and Equipment (3)

COMSEC material and equipment are items designed to secure or authenticate telecommunications. This includes, but is not limited to, keys, equipment, devices, documents, firmware or software that embodies or describes cryptographic logic or performs COMSEC functions. Information and material that are designated and marked are made available only to appropriately cleared personnel who have a legitimate need-to-know. COMSEC material and equipment are issued to and transferred only between COMSEC accounts. If further distribution is required, COMSEC custodians or alternates will issue the material or equipment on temporary "hand receipts." Hand receipts must be reissued every **6** months by the COMSEC custodian.

Communications Security (COMSEC) (A) (continued)

Control of COMSEC Material (4)

NRC COMSEC material will be controlled in accordance with current National Security Telecommunications and Information Systems Security (NSTISS) directives. COMSEC material consists of aids, equipment, components, and devices that are identifiable by the National Security Agency (NSA) telecommunications security nomenclature system. (a)

The NRC follows the **NSA** COMSEC accounting policies and procedures as prescribed in NSA Manual 90-2, "COMSEC Material and Control Manual," and Electronic Key Management System (EKMS) 702.01, "STU-III Key Management Plan." Copies of the above manuals are available to all NRC personnel assigned COMSEC responsibilities, or upon written request to the Director, **DFS.** (b)

Controlled Cryptographic Items (CCI) (5)

Controlled cryptographic items are secure telecommunications or information handling equipment or associated cryptographic components that are unclassified but governed by a special set of control requirements determined **by** the **NSA.** These items are marked "Controlled Cryptographic Item," or "CCI." CCI items are accounted for and controlled through the NSA COMSEC material control system (CMCS).

Other Materials (6)

Materials such **as** COMSEC instructional documents, COMSEC equipment operating and maintenance manuals, cryptographic ancillary material, are not cryptographic in scope, and are not marked "CRYPTO" or subject to the special safeguards required for information bearing that marking. However, for logistical control purposes, and as an identification aid to communications personnel, "non-crypto" COMSEC materials essential to secure communications are issued and transferred through the CMCS and made available only on a need-to-know basis. (a)

Communications Security (COMSEC) (A)(continued)

Other Materials (6) (continued)

Materials such as correspondence, messages, or publications, that are related to secure communications operations, but do not contain cryptographic information, are handled in accordance with the material classification or marking. Generally, all materials that mention or describe NRC secure communications facilities, operations, or capabilities, or that use short title designations of COMSEC material, require the minimum designation of "Official Use Only." (b)

Access to Cryptographic and COMSEC Information (7)

Certain U.S. classified cryptographic and/or COMSEC information, the loss of which could cause serious or exceptionally grave damage to **U.S.** national security, requires special access controls. ***An*** individual may be granted access to U.S. classified cryptographic information or COMSEC information, **only** if that individual-

- **Is** a **U.S.** citizen (a)
- Is an employee of the **U.S.** Government, is a **U.S.** Government-cleared contractor or employee of such contractor, licensee, certificate holder, or is employed as a U.S. Government representative (including consultants of the U.S. Government) (b)
- Possesses a security clearance appropriate to the classification level of the **U.S.** cryptographic information or COMSEC information to be accessed (c)
- Possesses a valid need-to-know as determined necessary to perform duties for, or on behalf of, the **U.S.** Government **(d)**
- Receives a security briefing appropriate to the U.S. cryptographic information or COMSEC information to be accessed (e)
- Acknowledges the granting of access by signing a cryptographic access or COMSEC access certificate ***(f)***

Communications Security (COMSEC) (A) (continued)

NRC Contractor COMSEC Authorizations (8)

Managers shall obtain Division of Facilities and Security (DFS), Office of Administration, authorization for either—(a)

- The release of operational COMSEC material to contractors, licensees, or certificate holders, for the purpose of transmitting classified information or data (i)
- The use of contractor personnel to install, maintain, or operate a secure communications facility for NRC (ii)

Managers also shall advise DFS of the start and termination of the actual use of such authorizations. **(b)**

COMSEC Functional Designations and Responsibilities (9)

COMSEC Control Officer (a)

The Chief, Information Security Branch (INFOSEC), DFS, is the COMSEC Control Officer for the agency and is responsible for the operation of the NRC Central Office of Record (COR) and for specifying control criteria for all COMSEC material.

Central Office of Record (b)

COR performs oversight of all NRC COMSEC accounts. COR coordinates all COMSEC activities with the National Security Agency (NSA) for NRC, particularly the accounting of all COMSEC material. (i)

COR periodically inspects all NRC COMSEC accounts. The Director, DFS, will send the cognizant organization any deficiency reports resulting from the inspection. The cognizant organization is responsible for correcting any deficiencies, just as it would implement recommendations from other security surveys or inspections. (ii)

The requirement to audit the NRC COR is vested in the NSA. NSA conducts these audits periodically and directs any resulting deficiency reports to the Director, DFS, for correction. NSA may audit individual COMSEC accounts at any time and provide resulting audit reports to the individual COMSEC accounts, with copies of deficiency reports to COR. (iii)

Communications Security (COMSEC) (A) (continued)

COMSEC Functional Designations and Responsibilities (9) (continued)

STU-III Command Authority (c)

The **STU-III** Command Authority is responsible for appointing, adding, deleting, or making changes to information regarding user representatives and their key ordering privileges. In most cases, user representatives are COMSEC custodians and alternates who order STU-III keying material for the secure telephones.

COMSEC Custodian (d)

The NRC currently has five COMSEC accounts, located at headquarters and each regional office. Each account has a primary custodian and **1** to **2** alternate custodians. COMSEC custodian duties include the receipt, transfer, accounting, safeguarding, and destruction of all COMSEC material assigned to the custodian's specific account. Managers shall nominate candidates in writing to the Director, **DFS,** and provide the individual's name, social security number **(SSN),** date of birth, place of birth, and security clearance or access authorization. COMSEC custodians must possess a "Q" clearance. The COR, after verification of clearance information, will appoint the COMSEC custodian in writing. Managers and candidates should be aware that there is a mandatory requirement for formal COMSEC custodian training upon assumption **of** COMSEC duties. When a change in custodian becomes necessary, the responsible manager shall submit a request for the change to the NRC COR at least **45** days in advance of the departure of the COMSEC custodian **to** allow for a change-of-custodian inventory to be conducted. If this is not possible, contact the COR for direction.

Alternate COMSEC Custodian (e)

Alternate COMSEC custodians assist the COMSEC custodian in the duties listed above. During periods when the COMSEC custodian is unavailable, the alternate custodian is authorized to perform these duties. Managers shall nominate candidates in writing to the Director, DFS and provide the individual's name, SSN, date of birth, place of birth, and clearance access level. Alternate COMSEC custodians must possess a **"Q"** clearance. The COR, after verification of clearance

Communications Security (COMSEC) (A)(continued)

COMSEC Functional Designations and Responsibilities (9) (continued)

information, will appoint the Alternate COMSEC custodian in writing. Managers and candidates should be aware that there is a mandatory requirement for formal COMSEC custodian training upon assumption of COMSEC duties.

Users ***(f)***

The individual user or holder of COMSEC material is personally responsible for the control and safeguarding of COMSEC material while it is entrusted to his or her care.

Installation of COMSEC Equipment (10)

Installation of Government-owned COMSEC equipment is subject to policies established by the National Security Telecommunications and Information Systems Security Committee (NSTISSC) and procedures set forth for the type **of** equipment involved. COMSEC equipment shall not be installed for new applications until all the following requirements have been met:

- Approved storage containers for the appropriate level of classified COMSEC material have been provided (a)
- The installation has been afforded the required physical safeguards and access controls (b)
- A security plan has been approved by Director, **DFS** ***(c)***

Acquisition of COMSEC Material (11)

All accountable COMSEC material, with the exception of the keying material for the secure telephone unit-generation three (STU-III), shall be controlled through the COMSEC CMCS. STU-III keying material shall be controlled through the NSA key management system **(KMS).** Contact your COMSEC custodian or the NRC COR to obtain both COMSEC material and STU-III keying material.

Communications Security (COMSEC) (A)(continued)

Releasing COMSEC Information to U.S. Contractors and Other Sources Outside the U.S. Government (12)

It should be noted that the release of COMSEC and COMSEC-related information, such as National Security Telecommunications and Information Systems Security Instructions (NTISSI) and National Communications Security Instructions (NACSI), to U.S. contractors and other U.S. non-governmental personnel is generally restricted. Any release of **NRC** COMSEC material to U.S. contractors and other U.S. non-governmental sources must be approved in advance by the Director, DFS.

Reporting COMSEC Insecurities (Incidents) (13)

The immediate reporting of any incident that may have subjected accountable classified COMSEC information furnished to NRC COMSEC accounts to be compromised is essential to ensuring the continued integrity of the information itself and the communications media protecting the information. In almost all cases, timely reporting of compromises to DFS will minimize the effects of the violation or loss of the information. The longer the delay in reporting incidents of security interest, the more difficult it becomes to determine and minimize the effect on national security. (a)

In reporting possible compromises to DFS and the NRC COR, the preferred mode of transmission is the STU-III, or successor equipment. When secure communications are not available, an unclassified report giving a brief unclassified description of the incident should be provided to DFS within 12 hours after discovery. After normal duty hours and on weekends and holidays, unclassified reports should be made to the Director, DFS, or the Chief, INFOSEC, through the NRC operator on 301-415-7000. (b)

In all cases, telephonic reports will be followed up by written correspondence, classified if appropriate, to Director, DFS, and, if accountable, COMSEC material is involved, also to the NRC COR. A followup written report detailing initial investigative actions and results should be submitted within 72 hours, and a final written report should be submitted within 30 days. Complete details of the incident and investigation are essential to determining the impact and followup actions necessary to minimize the effects of a compromise or security

Communications Security (COMSEC) (A) (continued)

Reporting COMSEC Insecurities (Incidents) (13) (continued)

violation and to draw a reasonable conclusion on the basis of fact. Each written report of a security incident involving COMSEC information should contain, as a minimum —(c)

- Name and address of the COMSEC account (i)
- Designated COMSEC custodian for the COMSEC account and the custodian's telephone number (ii)
- COMSEC account number (iii)
- Identification of the material involved (iv)
- Type of area control in effect (v)
- Description of the incident (vi)
- Personnel involved and their clearance levels (vii)
- Results of material inventory (viii)
- Investigative actions initiated and preliminary results (ix)
- Evaluation by the action officer of whether a compromise occurred (x)
- Actions taken to prevent recurrence of the incident (xi)

Followup and final reports will be classified a minimum of "CONFIDENTIAL-NSI" and should be marked "DECLASSIFY on: X1."

COMSEC Emergency Procedures (14)

Each organization holding classified or CCI COMSEC material must maintain, a current, written emergency plan for the protection of this material during emergencies. NSTISSI 4004, "Routine Destruction and Emergency Protection of COMSEC Material," dated March 11, 1987, or successor editions, provides guidance and information. Contact the COR to obtain a copy of the current document, or if additional information is required. These plans should be included in standard operating procedures and also should be posted as a separate document where it can be referenced by personnel during an emergency situation. The COMSEC emergency plans are approved by the COR and reviewed during COMSEC audits.

Secure Telecommunications Facilities Requirements (B)

Safeguarding COMSEC Facilities (1)

NRC-approved COMSEC facilities used for communicating National Security Information or Restricted Data shall be safeguarded in accordance with NSTISS directives. (a)

Cleared NRC personnel having a need-to-know, primarily as a result of their involvement in the supervision of the design, construction, or operation of an NRC COMSEC facility, may obtain copies of the applicable NSTISS directives upon written request to the Director, DFS. (b)

Establishment of a Secure Telecommunications Facility (2)

The feasibility and advisability of a secure telecommunications facility should first be established by preliminary communications with DFS. Once established, the NRC office requesting the telecommunications facility submits to DFS, for evaluation and approval, a security proposal for the facility, using the format provided in the exhibit of this handbook. Refer to NSTISSI **4005,** "Safeguarding COMSEC Facilities and Material," for minimum requirements for the construction and safeguarding of secure telecommunications facilities. Contact the Chief, INFOSEC, for a copy of this document. (a)

The proposal shall be developed only if a strong requirement exists for such a facility. Limitations on the number of secure facilities and the concentration of security measures at a centralized location is usually more prudent than creating multiple facilities. (b)

For NRC offices, OCIO and DFS will provide certain essential information for the proposal upon request, for example, floor plans, cryptographic equipment selections, and alarm designs. (c)

In each proposal, more detailed technical information may have to be elicited from the requesting office regarding the communicating techniques to be used. (d)

Secure Telecommunications Facilities Requirements (B) (continued)

Establishment of a Secure Telecommunications Facility (2) (continued)

When the security proposal is approved, it will become the facility communications security plan. It must be updated by the COMSEC Control Officer when modifications to the facility are proposed and must be resubmitted through the same process for approval. Copies of the plan, sound attenuation test reports, technical surveillance countermeasures (TSCM) reports, inspection reports, and TEMPEST test results, when required by ***NRC*** or other agencies, will be kept on file in DFS. (e)

Classified information may be discussed or transmitted only over those secure systems the Director, DFS, has approved in writing. ***(f)***

If more than one type of telecommunications system is desired for a single communications center, the user organization must submit only one proposal to the OCIO. If a telecommunications center also is to include the telecommunication of data from automated information systems *(AIS)*, the proposal should be written to cover all systems. Both DFS and OCIO are involved in the development of the proposal and the approval process for NRC users. See the guidelines for security proposals for AIS systems contained in Management Directive (MD) **12.5, "NRC** Automated Information Systems Security Program." (g)

Security Clearance for Installation, Maintenance, and Modification (3)

The installation, maintenance, and modification of a secure communications facility presents an opportunity for hostile penetration that may not be present when an encrypted signal is used. Ideally, all maintenance personnel should possess a final government issued security clearance. Personnel without a final security clearance may be used, but must be under constant visual observation by technically qualified and cleared NRC or NRC contractor personnel. A technical inspection must be conducted prior to the transmission of classified information. Uncleared persons must not have access to classified data transmitted via the system.

Secure Telecommunications Facilities Requirements (B) (continued)

Guidelines for Facility Design and Red/Black Installation (4)

Secure telecommunications systems must be installed in accordance with NSTISSAM TEMPEST 2-95, "Guidelines for Facility Design and Red/Black Installation," dated November 1, 1995. This document defines the guidance to consider during the design of facilities and for subsequent installation of equipment and systems that receive, transmit, manipulate, graph, store, archive, calculate, generate, print, or in any other manner, process national security information. Red/black installation recommendations, TEMPEST facility considerations, administrative support equipment (e.g., telephone systems, intercoms, alarms, and radio devices), cabling, inspectable space, and facility shielding are discussed in this document. Contact the Chief, INFOSEC, to obtain copies of this document.

Operation of Secure Telecommunications Facilities (C)

General Guidelines and Procedures (1)

There are numerous documents that provide guidance for the operation of secure telecommunications facilities from NSA and the NSTISSC. Contact the Chief, INFOSEC, to obtain copies of these documents.

Standard Operating Procedures (2)

The details for operating a telecommunications facility must be developed by the operating personnel under the direction of the COMSEC Control Officer on a case-by-case basis within the constraints imposed by the various NSA, NSTISSC, and NRC guidance documents.

Equipment Operation (3)

The operation of COMSEC equipment in NRC and NRC contractor systems must conform to NSA operations and maintenance manuals published for specific pieces of COMSEC equipment. Equipment that has been newly installed, relocated, or modified must not be operated until **DFS has** performed the required security checks of the operational

Operation of Secure Telecommunications Facilities (C)(continued)

Equipment Operation (3) (continued)

area. DFS-authorized qualified maintenance personnel also must check the equipment and determined that it is properly installed with all required modifications and ready for operation.

Handling of Information (4)

Classified and sensitive unclassified information shall be prepared, received, safeguarded, distributed, and disposed of in accordance with the requirements and procedures specified in MD 12.2, "NRC Classified Information Security Program," and MD 12.6, "NRC Sensitive Unclassified Information Security Program."

Security Surveys of Telecommunications Systems (5)

Telecommunications systems that receive, process, transmit, or safeguard classified data or information must be surveyed by DFS in accordance with the requirements and procedures of MD 12.1, **"NRC** Facility Security Program." The Director, DFS, shall furnish a statement of any proposed corrective actions resulting from the survey to the responsible headquarters office, division, regional office, or contractor. (a)

NRC COR inspections of all NRC COMSEC accounts will be performed periodically. The Director, DFS, will send the cognizant organization any deficiency reports resulting from the inspection for correction of the deficiency. The cognizant organization is responsible for correcting any deficiencies, just as it would implement recommendations from other security surveys or inspections. (b)

Followup of Deficiencies (6)

Managers shall ensure that their personnel follow up on any security deficiencies involving COMSEC or telecommunications systems. In turn, managers shall report any such matters to DFS, as required by this handbook.

Transmission and Emission Security (D)

Transmission Security (1)

Transmission security is the component of commynications security that results from the application of measures designed to protect transmissions from interception and exploitation by means other than cryptanalysis. To accomplish this, separation requirements are put into place to ensure classified information cannot be inadvertently transferred to unclassified transmission media and equipment. Red/black separation requirements and shielded cabling, along with the use of cryptographic equipment and technical surveillance counter-measures inspections at NRC, are the minimum recommended criteria for the design/installation of equipment within NRC controlled areas. Contact the Chief, INFOSEC, for additional information. (a)

Additional information regarding TSCM inspections can be found in MD **12.1.** (b)

Administrative telephones, intercom systems, and public address systems shall not be placed within **3** feet, and telephone wires or unclassified data communication lines shall not be placed within 1 foot, of a microcomputer system processing classified information or attached to a classified network. Communication lines, telephones, and other equipment and connections, in adjoining rooms, ceilings, and floors also are considered for purposes of distance separation. If it is necessary to have a telephone, telephone wires, intercom, or an unclassified data communication line closer than the minimum distances, the Director, DFS, must approve this in writing. (c)

Emission Security (2)

Emissions security is the protection resulting from measures taken to deny unauthorized persons information derived from intercept and analysis of compromising emanations from cryptographic equipment or an information system. (a)

All electronic equipment (e.g., microcomputers, typewriters, printers, scanners) emit electrical and electromagnetic radiation through the air or through conductors. The possibility exists that electronic eavesdroppers could intercept emanations, decipher them, and use this information to reconstruct the data being processed by the equipment, even being located some distance from the equipment. The use of TEMPEST-certified technology is the preferred method of protecting against compromising emanations. (b)

Transmission and Emission Security (D) (continued)

TEMPEST (3)

TEMPEST is an unclassified short name referring to investigations and studies of compromising emanations. Compromising emanations are unintentional intelligence bearing signals that, if intercepted and analyzed, will disclose classified information when it is transmitted, received, handled, or otherwise processed by any information processing equipment. (a)

Under certain circumstances and in some specific physical environments, non-TEMPEST telecommunications equipment may be used to communicate classified information when the Director, DFS, approves this in writing. (b)

Whether a specific piece of equipment can be used in certain cases in an unshielded environment must be determined on a case-by-case basis in the normal process of developing a security proposal. (c)

Technical Security Inspections (4)

DFS, will, upon request, arrange for technical security inspections such as TEMPEST and/or countermeasures inspections of secure telecommunications systems or facilities as dictated by local conditions or circumstances. (See MD 12.1 for additional information.)

Protection of Sensitive Unclassified Information (E)

Telecommunications Protection Authority (1)

The protection of sensitive unclassified information transmitted over telecommunications media (e.g., voice, video, network, facsimile, or other telecommunications systems) is required under National Security Decision Directive 145, "National Policy on Telecommunications and Automated Information Systems Security," and the Office of Management and Budget Circular A-130, "Management of Federal Information Resources." (a)

Protection of Sensitive Unclassified Information (E) (continued)

Telecommunications Protection Authority (1) (continued)

The procedures for the protection of sensitive unclassified information or data transmitted over telecommunications circuits used by any type of telecommunications system is given below. The general categories of sensitive unclassified that must be protected during ***NRC*** telecommunications transmissions are defined in MD **12.6,** and include Proprietary, Official Use Only, and Safeguards Information (SGI). **(b)**

Telecommunications Protection Procedures (2)

Record Telecommunications (a)

Record telecommunications include the telecommunication of data and information using network automated information systems and facsimile equipment. Telecommunications security for automated information systems must meet the requirements of MD 12.5. (i)

Sensitive unclassified record telecommunications using automated information systems, laptops, and/or facsimile systems must be transmitted over protected systems. Examples of protected systems include the following: (ii)

- Unclassified systems that use hardware or software implementations of the data encryption standard **(DES)** that the Director, DFS, has approved in writing. ***(a)***
- Unclassified systems that use hardware or software implementations of non-DES algorithms that the Director, **DFS,** has approved in writing. ***(b)***
- Other unclassified systems that the Director, **DFS,** has approved in writing. **(c)**
- Secure classified systems that use encryption equipment certified by NSA for the transmission of National Security Information and Restricted Data. ***(d)***

Protection of Sensitive Unclassified Information (E) (continued)

Telecommunications Protection Procedures (2) (continued)

Voice Telecommunications (b)

Sensitive unclassified voice telecommunications should be transmitted by protected systems to the maximum degree possible. The STU-III is the NRC-preferred telephone for the voice transmission **of** sensitive unclassified. Contact the Chief, INFOSEC, for the availability of STU-III telephones.

Privacy Act (c)

Managers shall ensure compliance with the provisions of MD **3.2,** "Privacy Act," if the information communicated or contained in the system is subject to the Privacy Act of 1974, as amended.

Secure Telecommunications Systems at NRC (F)

General (1)

Managers of NRC or NRC contractor telecommunications systems that process classified and/or sensitive unclassified information must ensure that personnel having access to the system are cognizant of and comply with the provisions **of** this handbook.

Security Proposals and Plans (2)

Managers shall obtain prior approval from DFS and OCIO for the operation of any telecommunications system by means of security proposals and plans.

Review of Telecommunications Traffic (3)

In conjunction with OCIO, and when requested by DFS, managers shall review the categories or subjects of unsecured clear voice radio and telephone traffic under their jurisdiction to determine whether any systems pass traffic of significant intelligence value. Managers shall furnish the results of these reviews to DFS through OCIO. **As** necessary, managers shall request OCIO to provide secure COMSEC equipment or privacy equipment.

Secure Telecommunications Systems at NRC (F) (continued)

Record Telecommunications (4)

Secure Facsimile (a)

All classified and sensitive unclassified information telecommunicated via facsimile must be transmitted over protected systems. The DFS's Secure Communications Center (COMCtr) provides secure facsimile service for the NRC headquarters, utilizing STU-III telephones for encryption. The Secure COMCtr operates daily during normal working hours. For emergencies, the DFS also has procedures for the receipt or transmission of information outside of normal working hours. In addition to the COMCtr, AEOD's Emergency Operations Center and each regional office has secure facsimile capability. The NRC Telephone Directory provides information on the locations and telephone numbers of secure facsimiles at NRC. (i)

Submit requirements for secure telecommunications equipment to the Director, DFS. Requests must clearly identify requirements and be appropriately justified. Ensure that no classified or sensitive unclassified data is included in the request. **DFS** will evaluate and verify each request and initiate the necessary procurement actions. **(ii)**

Automatic Digital Network (AUTODIN) (b)

The NRC DFS operates an AUTODIN system in the Secure COMCtr, Room O-2D6. The AUTODIN receives and transmits classified and unclassified messages within the Federal Government to include the Department of Defense; civil agencies (e.g., Federal Bureau of Investigations, Federal Emergency Management Agency, Department of Energy); embassies; and some non-governmental agencies such as the International Atomic Energy Agency (IAEA). Information received includes diverse national or international information or activities involving or relating to nuclear power or nuclear materials safety and safeguards, terrorist activities worldwide, threats and hostile actions against nuclear facilities, nuclear incidents worldwide, travel advisories, and IAEA international cooperation. (i)

Secure Telecommunications Systems at NRC (F) (continued)

Record Telecommunications (4) (continued)

AUTODIN is capable of sending and receiving classified and unclassified message traffic at various levels of classification and precedence categories. The Secure COMCtr operates daily during normal working hours, and DFS has procedures for emergencies. Contact the Information Security Branch for additional information on accessing this network. (ii)

Microcomputers (PCs) (c)

Any telecommunication of classified information, Safeguards Information (SGI), or sensitive unclassified information, using an AIS, whether network or standalone, must meet the requirements of MD 12.5.

Voice Telecommunications (5)

General (a)

Classified or sensitive unclassified voice telecommunications, whether by telephone, radio, video-teleconferencing, or another means, should be transmitted over protected systems to the maximum degree possible. The STU-III is the NRC-preferred telephone for voice transmission of classified and sensitive unclassified information. Submit requests for STU-III telephones in writing to the Director, DFS. Resident inspectors requesting secure voice capability should submit the request through the regional COMSEC custodian for concurrence. Requests for other secure telecommunications equipment should be submitted to the Director, DFS. (i)

Requests should include a point of contact, intended location of the STU-III telephone, anticipated number of users, and justification of the need for secure voice capability. Requests must clearly identify requirements and be appropriately justified. Ensure that no classified or sensitive unclassified data is included on the request. DFS will evaluate and verify each request and initiate the necessary procurement actions. (ii)

Secure Telecommunications Systems at NRC (F) (continued)

Voice Telecommunications *(5)* (continued)

Secure Telephone Unit-Third Generation (STU-III), Type 1 Terminal (b)

The STU-III is a self-contained secure analog telephone unit and data transmitter that fits on top of a desk. It uses public-switched telephone network circuits to establish an ordinary dial-up telephone communication path, then, by inserting a terminal-unique crypto-ignition key **(CIK)** into the telephone, and pushing the "Secure" button, can encrypt voice and data communications worldwide. There are over ***300,000*** STU-III telephones in use throughout the **U.S.** Government. The **Type 1** terminal has been endorsed by the NSA for securing classified or sensitive unclassified information, when appropriately keyed.

NRC Doctrine for the STU-III, Type 1, Telephone (i)

- The STU-III may be located in areas ranging from a true-type vault to a private office. The location must provide audio privacy to protect information being discussed. ***(a)***
- The STU-III must be inventoried daily or upon opening of the room where the telephone is located. The survey should consider signs of tampering and physical or cryptographic insecurities. Loss or possible compromise of the STU-III must be reported to the COMSEC custodian immediately, who then must report it to NRC COR. COMSEC custodians must conduct a physical sight inventory of all STU-III equipment annually, and should sight the equipment twice a year as part of the semiannual COMSEC inventory. *(b)*
- The STU-III is a CCI and must be protected in accordance with NSTISSI No. 4001, "Controlled Cryptographic Items." NRC requires that it also be protected as a high value item. **(c)**
- INFOSEC, will, upon installation of an STU-III provide any necessary training to the holders and users on the proper operation and protection of the STU-III Regional COMSEC custodians will provide training to their holders and users. It is the holder's responsibility to ensure that only those appropriately cleared individuals have access to the CIK. *(d)*

Secure Telecommunications Systems at NRC (F) (continued)

Voice Telecommunications (5) (continued)

- COMSEC custodians should periodically inspect STU-IIIs installed in locations accessed by unescorted cleaning crews or non-cleared personnel, for evidence of tampering. Any evidence of tampering must be reported to the Director, DFS, as a COMSEC incident, and the STU-III telephone must be removed from operation pending a determination by the proper authorities of the actions to be taken. ***(e)***
- When stored in the same room as the STU-III, CIKs must be placed in GSA-approved security containers. CIKs stored in areas apart from STU-III may be kept in a locked cabinet or desk drawer. Master CIKs are not provided to STU-III holders or users and will remain in the COMSEC custodian's custody at all times. **(f)**
- STU-III users should not normally keep CIKs in their personal possession (e.g., on a key ring or in a purse) or outside the building in which the corresponding STU-III is located. This course of action minimizes possible **loss of** CIKs and maximizes the availability of CIKs for authorized use. **(g)**
- CIKs must be placed in locked GSA-approved security containers in those areas in which cleaning crews have unescorted access. CIKs must never be left in an unattended STU-III, regardless of its location, and users must ensure that the CIK is secured after their calls are completed. ***(h)***
- At the end of each business day, the office to which the STU-III is assigned must ensure that **no** CIK is left in the STU-III overnight and that all CIKs are properly stored. *(i)*
- Any relocation of a STU-III terminal, whether temporary or permanent, must be reported to the COMSEC custodian, who then notifies the guard force of the relocation. If a STU-III is no longer required, contact the COMSEC custodian for disposition instructions. **(j)**

Secure Telecommunications Systems at NRC (F) (continued)

Voice Telecommunications (5) (continued)

- The STU-III telephone must be electronically rekeyed annually or when directed. At the present time, the annual electronic rekeying is performed by the COMSEC custodians. NSA recommends that the STU-III telephones be rekeyed more often, if possible. STU-III holders can perform electronic rekeying by inserting the CIK and turning it **1/4** clockwise; placing a call to EKMS (1-800-635-6301); and waiting until new operational key is downloaded. If any problems occur during rekeying, contact your COMSEC custodian for assistance. ***(k)***
- All COMSEC incidents related to the **loss,** compromise, or possible compromise of STU-III equipment or keys must be reported immediately by secure means to the NRC COR, which immediately reports to the Director, DFS. The Director, DFS, will determine any additional reporting requirements and take whatever reporting actions are necessary in accordance with existing NSA COMSEC reporting procedures. *(l)*

User Responsibilities (ii)

STU-III users are responsible for the proper use and control of their terminals and CIKs. Responsibilities include:

- Using the secure mode when discussing classified or sensitive unclassified information ***(a)***
- Closing the door to the room when using the telephone in the secure mode so that the conversation will not be overheard by persons without the need-to-know ***(b)***
- Adhering to the security classification displayed on the terminal for each call **(c)**
- When the terminal is keyed, limiting access to those with a proper clearance and need-to-know (d)
- Ensuring **only** those appropriately cleared individuals have access to the CIK **(e)**

Secure Telecommunications Systems at NRC (F) (continued)

Voice Telecommunications (5) (continued)

- Ensuring that the CIK is not left unattended in the STU-III terminal, and that the CIK is secured upon completion of the call **(f)**
- Checking the STU-III at the end of the day to ensure that a CIK has not been left in the unit and initialing the NRC Form 700 **(g)**
- Reporting COMSEC incidents to the COMSEC custodian or NRC COR. ***(h)***

Key Management (iii)

The policy for the management of Type 1 keying material is contained in EKMS 702.01, "STU-III Key Management Plan," and supplements published by **NSA.** Questions about NRC key management should be directed to the appropriate COMSEC custodian, the ***NRC*** COR, or the STU-III Command Authority. These offices and staff members maintain copies of the plan and supplements.

Hand-Receipts and Inventories (iv)

COMSEC custodians are required to perform semiannual inventories and issue hand-receipts to holders of COMSEC equipment.

STU-III Cellular (c)

The NRC has portable cellular STU-III briefcases that can transform desktop STU-IIIs into mobile units with cellular and land line transmission capability. Contact the appropriate COMSEC custodian or the NRC COR for additional information.

Exhibit

Format and Guidelines

for a

Secure Telecommunications Facility Proposal or Plan

Exhibit

Contents

Format and Guidelines for a Secure Telecommunications Facility Proposal or Plan . . . *27*
1 Introduction *27*
2 Secure Telecommunications *27*
2.1 Justification for the Need for Secure Telecommunications *27*
2.2 Duration and Nature **of** Activity *27*
2.3 Supplementary Glossary of Terms *28*
2.4 Equipment and Media *28*
2.5 System Functional Block Diagram *28*
2.6 Communications Security (COMSEC) *28*
3 Fixed COMSEC Facilities, Telecommunications Facilities. Secure Communications Centers 31
3.1 Physical Security 31
3.2 Access Lists 31
3.3 Visitor Control 31
3.4 Intrusion Alarm System/Protective Personnel 32
3.5 Protecting Passwords and Lock Combinations 32
3.6 Destruction 32
3.7 Floor Plans and Drawings 32
3.8 TEMPEST 33
3.9 Nonessential Audio/Visual Equipment 33
3.10 Technical Security Evaluation (TSE) 34
3.11 COMSEC Inspections 34
3.12 Unattended Secure Telecommunications Facilities 35
Attachment 36
Coordination Sheet 36

Exhibit

Format and Guidelines for a Secure Telecommunications Facility Proposal or Plan

1 Introduction

The format and guidelines cover the proposal requirements for both **NRC** contractors and NRC organizations.

If the proposed system contains a central'processingunit or a personal computer, it is also necessary to refer to Handbook **12.5,** "NRC Automated Information Systems Security Program," because such a system will be processing as well as transmitting classified data.

The complete proposal may be classified. It should be given a classification review and handled as classified in its draft form.

A coordination sheet should be attached to the front of the proposal and contain the appropriate coordination signatures (see the attachment to this exhibit).

2 Secure Telecommunications

Telecommunications systems prepare, transmit, communicate, or process information (e.g., writing, images, sounds) by electrical, electromagnetic, electromechanical, electro-optical or electronic means, using media such as telephone lines, cable, microwave, satellite, etc. Telecommunications systems include, but are not limited to, telephones, facsimiles, radios, video and video-teleconferencing, networks (e.g., LANs and WANs), or other data transmission systems.

Classified information may not be telecommunicated unless the telecommunications system has been approved by the Director, Division of Facilities and Security (DFS), Office of Administration. The ***NRC*** office requesting approval of a telecommunications facility must submit a security proposal using the format provided below. Submit the proposal to the Director, DFS, for evaluation and approval.

2.1 Justification for the Need for Secure Telecommunications

Justify the need for secure voice and/or data communications. Discuss the classification levels (e.g., secret or confidential); categories of information (e.g., national security information (NSI) or restricted data (RD)); and the types of information (e.g., material control and accountability information) being transmitted.

2.2 Duration and Nature of Activity

Indicate if this is an ongoing requirement or if short-term and the probable duration of the telecommunications activity.

Exhibit (continued)

Format and Guidelines for a Secure Telecommunications Facility Proposal or Plan

(continued)

2.3 Supplementary Glossary of Terms

Define any special terminology applicable to the telecommunications system that may be system-unique or not defined in NSTISSI 4009, "National Information Systems Security (INFOSEC) Glossary."

The terms "Secure Communications Center" and "Telecommunications Facility," refer to a type of facility dedicated to the preparation, transmission, communication or related processing of information. Unless otherwise noted, both terms refer to both attended and unattended facilities.

2.4 Equipment and Media

List all equipment and media that comprises the secure telecommunications system, including terminal equipment, cryptographic equipment, modems, switching systems, signaling equipment, and testing equipment. If the telecommunications system is to be networked, describe the network media used, e.g., twisted pair cable, coaxial cable, fiber optic cable, microwave, satellite, or combinations of media (e.g., a network system that uses Ethernet cabling throughout a building, but fiber optic cabling between buildings).

Provide the manufacturer's name and the model number of each piece of equipment.

2.5 System Functional Block Diagram

By means of a complete system functional block diagram, show the functional interrelationship of all equipment associated with the secure telecommunications system, including terminal equipment, cryptographic equipment, and modems. If the telecommunications system is to be networked, provide the network security architecture, specifically addressing security-relevant issues. All interconnected nodes on the network should be provided on the block diagram. Provide a brief narrative description, as necessary, to supplement the diagram.

2.6 Communications Security (COMSEC)

COMSEC is a program in which the National Security Agency (NSA) acts as the central procurement agency for the development and, in some cases, the production of INFOSEC items. The NSA certifies cryptographic and other communications security products such as key, equipment, devices, documents, firmware, or software that

Exhibit (continued)

Format and Guidelines for a Secure Telecommunications Facility Proposal or 'Plan

(continued)

embodies or describes cryptographic logic or performs COMSEC functions. COMSEC is considered especially sensitive because of the need to safeguard **U.S.** cryptographic principles, methods, and material against exploitation.

2.6.1 COMSEC Accounts

COMSEC accounts are administrative entities, identified by an account number, used to maintain accountability, custody, and control of COMSEC material.

Discuss the COMSEC account(s) that exists or is planned. Provide the name, address, and telephone number of the Central Office of Record (COR) of the COMSEC account (if already established). Discuss the contents of the COMSEC account inventory in general terms only (e.g., the holdings in this account include the secure telephone units **[STU-IIIs],** Type 1 seed key, traditional key, electronic key, **KG-84s,** and the data encryption standard key). If additional information is required, the NRC will contact the COR of the account.

NOTE: Not all equipment and material associated with a telecommunications system is COMSEC accountable and this equipment may be different than the equipment listed in Section **2.4.**

2.6.2 COMSEC Custodians and Alternates

Designate the names, titles, and qualifications (citizenship, possess a valid **"Q"** clearance, COMSEC or related experience, training) of the individuals who have been selected as the COMSEC custodian and alternate(s).

Because of the sensitivity of COMSEC material and the rigid controls required, the COMSEC custodian and alternate(s) must possess exemplary qualities. Ensure that the individuals selected:

- Are responsible individuals qualified to assume the duties and responsibilities of a COMSEC Custodian
- Are in a position or level **of** authority that will permit them to exercise proper jurisdiction in fulfilling their responsibilities
- Have not been previously relieved of COMSEC custodian duties for reasons of negligence or nonperformance of duties

Exhibit (continued)

Format and Guidelines for a Secure Telecommunications Facility Proposal or Plan

(continued)

- Are in a position that will permit maximum tenure (not less than **1** year)
- Will not be assigned duties that will interfere with their duties as COMSEC custodian or alternate
- Are actually performing the custodial functions on a day-to-day basis (The COMSEC custodian position will not be assumed solely for the purpose of maintaining administrative or management control of the account functions.)
- Hold grade **GG-7** or above

2.6.3 COMSEC Material Accountability

Describe how the accountability of COMSEC materials and documents is maintained (e.g., under NRC oversight, the Department of Energy (DOE) oversight, or NSA oversight).

2.6.4 Storage, Transportation, Reproduction, and Destruction of COMSEC Material

National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 4005, "Safeguarding COMSEC Facilities and Material," establishes the minimum national standards for safeguarding COMSEC material.

Describe how COMSEC material is/or will be stored, transported, reproduced, protected, and destroyed. In the case of destruction of accountable COMSEC documents and keying material, state the type, manufacturer, and model number of any destruction equipment (e.g., shredders) you would like to have considered by the Director, DFS, as approved equipment. Describe the techniques used in the destruction process (e.g., mixture of classified material with unclassified material, and the method of disposal **of** the waste material).

2.6.5 COMSEC Training

Discuss COMSEC training (e.g., **ND-112,** NSA COMSEC Custodian Course) previously received (include dates) by COMSEC custodian or alternates (e.g., DOE COMSEC training or NSA COMSEC training). Indicate the number of people requiring training, the approximate timing for such training, and the name and title of the individual who will coordinate the training.

Exhibit (continued)

Format and Guidelines for a Secure Telecommunications Facility Proposal or Plan

(continued)

3 Fixed COMSEC Facilities, Telecommunications Facilities, Secure Communications Centers

NSTISSI 4005 establishes the minimum national standards for constructing and protecting COMSEC facilities, wherein the primary purpose is generating, storing, repairing, or using COMSEC material.

Work areas not considered COMSEC facilities that contain COMSEC equipment (e.g., STU-IIIs, **KG-84s,** and/or data transfer devices) must be protected in a manner that affords protection at least equal to what is normally provided to other high value and sensitive material and ensure that access and accounting integrity is maintained.

3.1 Physical Security

Describe the physical location of the facility within its host building. Discuss the functions and relative locations of adjacent buildings and rooms. Describe the construction of the facility, to include walls, floors, ceilings, main entrance door, other doors, door locks, windows, other openings, and security systems in place (e.g., intrusion alarms, armed guards, and/or video cameras).

Describe the procedures for daily security checks (e.g., visual checks are made at least once every **24** hours on a random basis by personnel assigned to the facility).

Provide initial and latest reinspection reports, technical security evaluation (TSE) report, and TEMPEST countermeasures and verification reports, if applicable.

3.2 Access Lists

Discuss requirements for access to the secure facility. Include the functional titles of the individuals who will routinely access the facility. Provide the title of the official who will generate the access lists and the method to be used for keeping the list up to date.

3.3 Visitor Control

A visitor register must be maintained at the facility entrance area to record the arrival and departure of authorized visitors. Describe the format of the log, requirements for the monitoring of visitors while in the facility, how personnel security clearances are verified, and what personal identification is required for access to the facility.

Exhibit (continued)

Format and Guidelines for a Secure Telecommunications Facility Proposal or Plan

(continued)

3.4 Intrusion Alarm System/Protective Personnel

Describe the type of intrusion alarm system (e.g., infrared, ultrasonic) used to protect the facility and where the alarm annunciates. Specify the required response time of protective personnel, if the alarm is activated.

3.5 Protecting Passwords and Lock Combinations

Describe the method used for protecting combinations for the secure facility. Refer to NSTISSI 4005 for the requirements for controlling the combinations of containers used to store COMSEC documents and material. Describe the written instructions furnished to the secure facility's personnel and users for controlling combinations.

3.6 Destruction

Identify the pertinent types of classified media (e.g., printed or magnetic storage media) involved in the activities of the secure facility and the classification of the media (e.g., Secret-National Security Information, Secret-Restricted Data).

Describe the methods of both routine and emergency destruction of each type of media (e.g., shredding, degaussing). See NSTISSI 4004, "Routine Destruction and Emergency Protection of COMSEC Material (U)," for guidance in the destruction of COMSEC material.

3.7 Floor Plans and Drawings

Provide the following:

Floor plans of the secure facility showing the location of all equipment, including all terminals, related cryptographic equipment, modems, and other telecommunications equipment

- Floor plans showing the construction of walls, floor, and ceiling of the room(s) containing the secure equipment
- Separate architectural details such as doors, windows, and ducts
- Floor plans that indicate the type of facilities and operations in the areas adjacent to and on the floors immediately above and below the secure facility and installation drawings, including wiring diagrams and conduit plans for the secure telecommunications equipment

Exhibit (continued)

Format and Guidelines for a Secure Telecommunications Facility Proposal or Plan

(continued)

3.8 TEMPEST

"TEMPEST" is an unclassified short name referring to investigations and studies of compromising emanations. Compromising emanations are unintentional intelligence-bearing signals that, if intercepted and analyzed, will disclose classified information when transmitted, received, handled, or otherwise processed by any information processing equipment.

TEMPEST countermeasures will be applied only in proportion to the threat of exploitation and the resulting damage to the national security, should the information be obtained by a foreign intelligence organization.

Identify what TEMPEST countermeasures may be required for the secure facility. If TEMPEST countermeasures are in use at the facility, describe your implementation of the program (e.g., certification, accreditation, zoning, shielding).

3.9 Nonessential Audio/Visual Equipment

Certain **U.S.** Government-owned **or** -leased (or company-owned or -leased) items are prohibited in secure facilities unless approved by the Director, DFS, for conduct of official duties. These include two-way transmitting equipment, recording equipment (audio, video, optical), and test, measurement, and diagnostic equipment. *Also*, certain personally owned electronic equipment items, such as photographic, video, and audio recording equipment; and computers and associated media, are prohibited in secure facilities.

Describe in the plan any telephone, intercom, paging, or music systems that are internal to, or penetrate the secure facility. Verify and certify that there are no fortuitous conductors, speakers that can be reversed to be used as microphones, or telephones that can be rewired to be used as microphones. Pay particular attention to any wire penetrations into the secure facility by any system operated or controlled from outside the facility. This section **of** the plan also should describe the controls and restrictions imposed on personnel bringing electronic devices into the secure facility.

Exhibit (continued)

Format and Guidelines for a Secure Telecommunications Facility Proposal or Plan

(continued)

3.10 Technical Security Evaluation (TSE)

All reasonable countermeasures should be taken to ensure that there are no clandestine surveillance devices in secure telecommunications facilities. Evaluations for clandestine surveillance devices should be conducted as appropriate to the threat level determined by the Director, DFS. These evaluations should be considered when facilities are initially activated or reactivated after foreign occupation, or when there is known or suspected access by foreign maintenance or construction personnel, or when clandestine surveillance or recording devices are suspected in or near a secure facility. Any actual or suspected clandestine surveillance or recording devices must be reported in accordance with the requirements of NSTISSI **4003,** "Reporting and Evaluating COMSEC Incidents."

Describe any tests **or** inspections of the secure facility that are planned or have already been performed. Indicate the frequency of the testing, the reason for the frequency (e.g., type, purpose, and classification level of the information handled at the secure facility, or specific equipment contained therein), and if the tests and inspections include external sound attenuation tests and audio countermeasure tests to detect clandestine "eavesdropping" devices.

Provide a list of tests to be performed, copies of the specific test procedures to be used, and the name **of** the contractor(s) performing the tests to the Director, DFS, for approval. If the tests have already been conducted, provide a copy of the test results to the Director, DFS, for approval.

3.11 COMSEC Inspections

A COMSEC inspection should be conducted prior to initial activation where practical, but must be conducted within **90** days after activation. Thereafter, facilities must be reinspected based on threat, physical modifications, sensitivity of programs, and past security performance. At a minimum, the inspection must address secure operating procedures and practices, handling and storage **of** COMSEC material, and routine and emergency destruction capabilities.

Describe the procedures, either in place or planned, for conducting COMSEC inspections.

Exhibit (continued)

Format and Guidelines for a Secure Telecommunications Facility Proposal or Plan

(continued)

3.12 Unattended Secure Telecommunications Facilities

Unattended secure telecommunications facilities must be protected by an intrusion detection system or guarded in accordance with NSTISSI 4005.

Describe any special security controls in place for unattended secure telecommunications facilities. Information on response time to an alarm, storage of keyed COMSEC equipment and maintenance manuals, procedures for inspection of the facility, and emergency procedures, should be addressed in the plan.

Attachment

Coordination Sheet

_____
Director of Facilities and Security
Office of Administration

_____
Director, Division of Contracts and
Property Management, ADM

_____ or _____
Director, Division of Regional Administrator

_____
Prepared by

U.S. NUCLEAR REGULATORY COMMISSION

DIRECTIVE TRANSMITTAL

TN: DT–99–03

To: NRC Management Directives Custodians

Subject: Transmittal of Directive 12.5, "NRC Automated Information Systems Security Program"

Purpose: Directive and Handbook 12.5 are being revised for clarity and to reflect organizational changes within NRC. The Office of Management and Budget (OMB) issued a revised Circular A-130, Appendix III, "Security of Federal Automated Information Resources," which is the basis for the NRC computer security program. Handbook 12.5 has been updated to reflect the changes necessitated by the revision of OMB Circular A-130 and by other changes in the processing environment.

Office and Division of Origin: Office of the Chief Information Officer

Contact: Louis H. Grosman, 415–5826

Date Approved: May 2, 1995 (**Revised: February 1, 1999**)

Volume: 12 Security

Directive: 12.5 NRC Automated Information Systems Security Program

Availability: Rules and Directives Branch
Office of Administration
David L. Meyer (301)415–7164 or
Jeannette P. Kiminas (301)415–7086

NRC Automated Information Systems Security Program

Directive 12.5

Contents

Policy 1

Objectives 1

Organizational Responsibilities and Delegations of Authority 1

Chief Information Officer (CIO) 1

Director, Division of Facilities and Security (DFS), Office of Administration (ADM) 2

Director, Division of Contracts and Property Management (DCPM), ADM 3

Associate Director for Training and Development, Office of Human Resources (HR) 3

Office Directors and Regional Administrators 3

Applicability 4

Handbook 4

Exceptions 4

References 5

NRC Automated Information Systems Security Program Directive 12.5

Policy
(12.5–01)

It is the policy of the U.S. Nuclear Regulatory Commission to maintain an automated information systems (AIS) security program to provide appropriate administrative, technical, and physical security measures for the protection of the agency's AIS facilities, AIS, and information commensurate with the risk and harm resulting from the loss, misuse, or unauthorized access to these information resources.

Objectives
(12.5–02)

To implement appropriate security measures for the protection of NRC general support systems, major applications, and systems processing classified, unclassified safeguards information, and sensitive unclassified information and to adequately protect the information processed and stored in such systems.

Organizational Responsibilities and Delegations of Authority
(12.5–03)

Chief Information Officer (CIO)
(031)

- Develops, manages, and implements policies and procedures for the NRC AIS security program. (a)
- Ensures, through coordination with the Personnel Security Branch (PERSEC), Division of Facilities and Security (DFS), Office of Administration (ADM), that individuals designated to participate in the design, planning, operation, or maintenance of sensitive NRC

Chief Information Officer (CIO)
(031) (continued)

AIS and/or having access to sensitive data are properly screened and eligible for access to this information or these systems in accordance with the personnel security requirements contained in Management Directive (MD) 12.3, "NRC Personnel Security Program." (b)

- Ensures, in conjunction with DFS, the adequacy of personnel security requirements included in contracts, interagency agreements, and designs for NRC AIS and applications programs. (c)
- Appoints, with the concurrence of DFS, the Observer and the Alternate Observer for the Subcommittee for Information Systems Security (SISS) of the National Security Telecommunications and Information Systems Security Committee (NSTISSC). (d)
- Reviews and approves risk analysis results, security plans, and contingency plans for general support systems and major applications. (e)
- Adheres to the responsibilities of Section (035) of this directive. (f)
- Provides guidance and assistance to other NRC user organizations implementing all aspects of this directive and handbook. (g)

Director, Division of Facilities and Security (DFS), Office of Administration (ADM)
(032)

- Coordinates, reviews, and approves, in conjunction with OCIO, security proposals and plans originated by NRC organizations, licensees, and contractors for AIS and AIS facilities that process classified information. (a)
- Reviews, concurs in, and may contribute security requirements for the implementation of AIS or AIS facilities and feasibility studies for AIS or AIS facilities that process classified information. (b)
- Approves cryptographic hardware and software solutions for protection of information systems that process classified information. (c)
- Ensures that facility planning and installation are provided for all NRC AIS that process, store, or produce classified information. (d)

Director, Division of Contracts and Property Management (DCPM), ADM
(033)

- Ensures that all Federal and NRC requirements for the protection of classified, safeguards, or sensitive unclassified information are provided in solicitations and contracts involving automated systems processing such information. (a)
- Ensures that the requirements of DCPM Instruction 94-3, "Incorporation of Security Requirements for Information Technology (IT) Services," Revision 1, August 29, 1997, are implemented for all information technology acquisitions. (b)
- Ensures that procurement requests for AIS involving classified, safeguards, or sensitive unclassified information have received the appropriate level of coordination with DFS and OCIO. (c)

Associate Director for Training and Development, Office of Human Resources (HR)
(034)

- Provides assistance in the development and delivery of appropriate computer security training programs for NRC personnel who work on NRC AIS that process or produce classified, safeguards, or sensitive unclassified information as specified in the handbook to this directive. (a)
- Provides other computer security-related training as requested. (b)
- Ensures that a computer security briefing is included in the initial orientation of new employees. (c)

Office Directors and Regional Administrators
(035)

- Identify all general support systems, major applications, and other systems processing classified, safeguards, or sensitive data for which his or her office is the sponsor and implement the security controls for the identified systems required by OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources," and in accordance with the guidance in Handbook 12.5. (a)
- Ensure that all AIS sponsored by his or her office and operated by NRC or NRC contractors comply with the requirements of this directive and handbook. (b)

Office Directors and Regional Administrators
(035) (continued)

- Ensure that all Federal and NRC requirements for the protection of classified, safeguards, or sensitive unclassified information are provided in solicitations and contracts involving automated systems processing such information. (c)

- Ensure that the requirements of DCPM Instruction 94-3 are implemented for all information technology acquisitions. (d)

Applicability
(12.5–04)

This directive and handbook apply to all NRC employees, consultants, experts, panel members, contractors, and subcontractors, as applicable, who own, manage, or operate an AIS facility or process, store, or produce classified, safeguards, or sensitive unclassified information on AIS that are under the security jurisdiction of the NRC, including those individuals performing work for the NRC pursuant to interagency agreements, memoranda of understanding, or financial assistance programs. The National Industrial Security Program Operating Manual contains the applicable security regulations for contractors involved with classified AIS.

Handbook
(12.5–05)

Handbook 12.5 contains the procedures to implement an AIS security program to provide administrative, technical, and physical security measures for the protection of all AIS facilities, AIS, and classified, safeguards, or sensitive unclassified information processed, stored, or produced in AIS.

Exceptions
(12.5–06)

Exceptions or deviations to this directive and handbook may be granted by OCIO, except for those areas in which the responsibility or authority is vested solely with the Commission, the Executive Director for Operations, or ADM and is not delegable, or for matters specifically required by law, Executive order, or directive to be referred to other management officials.

References
(12.5–07)

Computer Fraud and Abuse Act of 1986, as amended, Pub. L. 99-474 (18 U.S.C. 1001 note).

Computer Security Act of 1987, Pub. L. 100-235 (40 U.S.C. 739 note).

Division of Contracts and Property Management Instruction 94-3, Revision 1, "Information of Security Requirements for Information Technology (IT) Services," August 29, 1997.

Federal Managers' Financial Integrity Act of 1982 (31 U.S.C. 3512 et seq. and 31 U.S.C. Chapter 11).

National Industrial Security Program Operating Manual (NISPOM), U.S. Department of Defense, October 1, 1994.

National Institute of Standards and Technology (NIST), Federal Information Processing Standards (FIPS) Publication 46-2, "Data Encryption Standard," December 30, 1993.

— FIPS Publication 87, "Guidelines for ADP Contingency Planning," March 27, 1981.

— FIPS Publication 102, "Guideline for Computer Security Certification and Accreditation," September 27, 1983.

— FIPS Publication 112, "Standard on Password Usage," May 30, 1985.

— Special Publication 800-4, "Computer Security Considerations in Federal Procurements: A Guide for Procurement Initiators, Contracting Officers, and Computer Security Officials," March 1992.

— Special Publication 500-109, "Overview of Computer Security Certification and Accreditation," April 1984.

— Special Publication 500-153, "Guide to Auditing for Controls and Security," April 1988.

— Special Publication 500-172, "Computer Security Training Guidelines," November 1989.

References
(12.5–07) (continued)

National Institute of Standards and Technology Internal Report (NISTIR) 4749, "Sample Statements of Work for Federal Computer Security Services: for Use In-House or Contracting Out."

NRC Management Directive—

2.5, "NRC Information Systems Development Life Cycle Management."

4.3, "Financial Management Systems."

11.7, "NRC Procedures for Placement and Monitoring of Work With the U.S. Department of Energy (DOE)."

12.2, "NRC Classified Information Security Program."

12.3, "NRC Personnel Security Program."

12.4, "NRC Telecommunications Systems Security Program."

12.6, "NRC Sensitive Unclassified Information Security Program."

13.1, "Property Management."

NRC Management Directive System Volume 12, "Security," contains a Glossary of terms applicable to the volume.

NRC, "The Nuclear Regulatory Commission's Procedures for Use of the U.S. Government Bankcard," Office of Administration, October 1998.

NUREG/BR-0166, "Instructions for Preparing Security Plans for Local Area Networks in Compliance With Office of Management and Budget (OMB) Bulletin No. 90-08," February 1992.

NUREG/BR-0167, "Software Quality Assurance Program and Guidelines," February 1993.

NUREG/BR-0168, "Security Policy for Processing and Handling of Sensitive Unclassified Information in the AUTOS/Local Area Network Environment," Rev. 1, November 1994.

References

(12.5–07) (continued)

Office of Management and Budget Bulletin 90-08, "Guidelines for Writing Security Plans Mandated by the Computer Security Act of 1987," July 9, 1990.

— Circular A-123, "Management Accountability and Controls," June 21, 1995.

— Circular A-127, "Financial Management Systems," July 23, 1993.

— Circular A-130, Transmittal Memorandum No. 3, "Management of Federal Information Resources," Appendix III, "Security of Federal Automated Information Systems," February 8, 1996.

"U.S. Department of Commerce Abbreviated Certification Methodology Guidelines for Sensitive and Classified Information Technology Systems," December 1, 1992.

NRC Automated Information Systems Security Program

Handbook 12.5

Contents

Part I

The NRC Automated Information System (AIS) Security Program 1

Protection of Systems (A) 1

Legal Foundations for Federal Computer Security (1) 1

Responsibilities (2) 2

Systems Requiring Protection (3) 3

System Protection Requirements (4) 5

User Responsibilities (B) 7

System Security Officer (C) 9

Information Classification and Sensitivity Level (D) 10

Risk Assessment (E) 12

System Security Plan (SSP) (F) 14

Contingency Plan (G) 15

Certification (H) 17

System Certification (1) 17

Software Certification (2) 18

Security Specifications (3) 18

Accreditation (I) 19

Accreditation Authority (1) 19

Memorandum of Accreditation/Non-Accreditation (2) 20

Accreditation Authority Signature (3) 20

Reaccreditation (4) 20

Interim Authority To Operate (5) 21

Accreditation Tracking (6) 21

Contents (continued)

Part II

Automated Information System (AIS) Security Controls 22

Physical Security of AIS Assets (A) 22

Computer Room and AIS Equipment Room Physical Security Controls (1) . 22

Workstation Physical Security Controls (2) 24

Network Physical Security Controls (3) 24

Key and Combination Control Procedures (4) 25

Environmental Security Controls (B) 26

Housekeeping (1) 26

Fire Protection (2) 27

Protection From Water Damage (3) 27

Power Protection (4) 27

Administrative Security Controls (C) 27

Individual Use of AIS (1) 27

Management of User Identifications and Passwords (2) 27

Telecommuting, Flexible Workplace, and Remote Access (3) 29

Security of Portable Computers (4) 29

Electronic Mail (5) 30

Reporting Incidents and System Anomalies (6) 30

Investigating Incidents (7) 30

Warning Banner (8) 31

Inventory of Applications (9) 32

Asset Inventory (10) 32

Configuration Management (11) 32

Visitor Control (12) 33

Virus Controls (13) 33

Contents (continued)

Part II (continued)

Personnel Security Controls (D) 33
Personnel Security Principles (1) 34
Position Definition (2) 34
Personnel Screening (3) 34
Termination of Access Rights (4) 35
Nondisclosure of Information (5) 36
System Security Controls (E) 36
General (1) 36
Identification and Authentication (I&A) Controls (2) 37
Specific Password Controls (3) 38
User-Defined Password Standard (4) 38
Discretionary Access Controls (5) 39
Auditing Controls (6) 40
System Integrity Controls (7) 41
Data Integrity Controls (8) 42
Reliability of Service Controls (9) 42
Telecommunications Security Controls (F) 42
General Network Security Guidelines (1) 42
Dial-Up Security Guidelines (2) 44
Guidelines for Internet Security (3) 46
Information Security Controls (G) 50
Documentation (1) 50
Backup of AIS (2) 50
Labeling of AIS Media (3) 52
Storage of AIS Media (4) 54
Destruction of Storage Media (5) 55

Contents (continued)

Part II (continued)

Security Controls for AIS Processing SGI or Classified Data (H) 56

Security Controls for AIS Processing Unclassified SGI (1) 56

Security Controls for AIS Processing Classified Information (2) 57

Abbreviations 60

Glossary 62

Exhibits

1 Determining Protection Requirements for Automated Information Systems (AIS) 76

2 Application Recovery Capabilities 77

3 NetWare Security 81

4 Windows NT Security 85

5 UNIX Security 87

6 AUTOS Remote Access Agreement 93

Part I

The NRC Automated Information System (AIS) Security Program

Protection of Systems (A)

The NRC AIS Security Program is designed to ensure that adequate protection is provided for NRC General Support Systems, Major Applications, and systems that are used to process, transmit, or store sensitive unclassified, safeguards, or classified information. This part addresses responsibilities for protecting these systems, identification of systems to be protected, and minimum system protection requirements.

Legal Foundations for Federal Computer Security (1)

- The Computer Security Act of 1987 requires agencies to identify sensitive systems, conduct computer security training, and develop computer security plans. (a)
- Office of Management and Budget (OMB) Circular A-130 (specifically Appendix III, "Security of Federal Automated Information Resources") requires Federal agencies to establish security programs containing specified elements. (b)
- Executive Order 12958, "Classified National Security Information," October 16, 1995. (c)
- Unclassified safeguards information (SGI) is controlled in accordance with Section 147 of the Atomic Energy Act of 1958, as amended and 10 CFR 73.21. (d)

Protection of Systems (A) (continued)

Responsibilities (2)

System Sponsor (a)

NRC offices that sponsor systems in the categories defined in Section (A)(3) of this part, are responsible for ensuring that appropriate security controls are implemented for such systems. This includes implementation of the security controls identified in OMB Circular A-130, Appendix III, and in system protection requirements and evaluating the security posture of these systems on a recurring basis (see Section (A)(4) of this part). Additionally, system sponsors will periodically identify systems according to the sensitivity level of data processed by the system in accordance with system classification and sensitivity level (see Section (D) of this part).

Office of the Chief Information Officer (OCIO) (b)

The OCIO has primary responsibility for developing, managing, and implementing policies and procedures for the protection of NRC General Support Systems, Major Applications, or other systems that are used to process, transmit, or store sensitive unclassified, safeguards, or classified information. The OCIO will provide guidance and assistance to the system sponsor in developing and evaluating the security of their individual systems. OCIO responsibilities in assuring appropriate system protection include:

- Reviewing and approving security plans and business continuity plans for NRC general support systems, major applications, and AIS processing classified, safeguards, or sensitive unclassified information, as well as reviewing and approving all modifications to such plans. (i)
- Providing guidance and assistance to system sponsors to develop the necessary security plans and business continuity plans for AIS that require protection. (ii)
- Conducting periodic and special reviews to determine the vulnerabilities and the adequacy and effectiveness of protective measures for NRC AIS requiring protection (see Section (A)(3) of this part). (iii)
- Conducting periodic agencywide surveys to identify all new AIS requiring protection and maintaining an inventory of such systems. (iv)

Protection of Systems (A) (continued)

Responsibilities (2) (continued)

- Providing virus protection and eradication services. (v)
- Conducting activities to ensure an appropriate level of computer security awareness among NRC staff. This includes providing periodic computer security awareness training for NRC headquarters and regional staff; conducting additional computer security awareness briefings for small groups as requested; conducting computer security awareness training for new employees; and coordinating the annual NRC observance of International Computer Security Awareness Day. (vi)
- Determining, in conjunction with the Division of Facilities and Security (DFS), Office of Administration, requirements for cryptographic hardware and software solutions for AIS requiring such protection. (vii)
- Acting on recommendations pertaining to computer security from DFS resulting from facility security surveys, assessments of AIS, and/or guidance to the AIS user. (viii)
- Notifying DFS of a suspected compromise or unauthorized access or misuse of a system. (ix)
- Reviewing, commenting on, and concurring in changes to Management Directive (MD) 12.4, "NRC Telecommunications Systems Security Program." (x)
- Maintaining and updating this directive and handbook. (xi)

Systems Requiring Protection (3)

General Support Systems (a)

A general support system is an interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, and people. This includes local-area networks (LANs), wide-area networks (WANs), servers, and data processing centers. OMB Circular A-130, Appendix III, requires the establishment of security controls in all general support systems, under the presumption that all contain some sensitive information. These systems are to be identified by the NRC sponsor and will be covered by an individual security plan. The system

Protection of Systems (A) (continued)

Systems Requiring Protection (3) (continued)

sponsor is responsible for ensuring that security controls are applied in accordance with the requirements contained in OMB Circular A-130, Appendix III, and described in Section (A)(4) of this part.

Major Applications (b)

The term means a *computerized* information system or application that requires special attention to security because of the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. These applications require special management oversight. For example, an agencywide financial management system containing NRC's official financial records would be a major application requiring its own security plan. A local program designed to track expenditures against an office budget would not be considered a major application and would be covered by a general support system security plan (SSP) for an office automation system or a LAN. Standard commercial off-the-shelf software (such as word processing software, electronic mail software, utility software, or general purpose software) would not typically be considered a major application and would be covered by the plans for the general support system on which they are installed. (i)

OMB Circular A-130, Appendix III, advises that agencies are expected to exercise management judgment in determining which of their applications are major and focus security controls on the identified limited number of particularly high-risk or major applications. These systems are to be identified by the NRC system sponsor and covered by an individual security plan. The system sponsor is responsible for ensuring that security controls are applied in accordance with the requirements contained in OMB Circular A-130, Appendix III, and described in Section (A)(4) of this part. (ii)

Non-Major Application Systems Processing Sensitive Data, Unclassified Safeguards Data, or Classified Data (c)

Systems used to process sensitive data, as defined in the Glossary of Volume 12, "Security," of the Management Directive System (MDS) and SGI or classified data are to be identified by the NRC system sponsor and will be covered by an individual security plan. The system sponsor is responsible for ensuring that security controls are applied in accordance with the requirements contained in OMB Circular A-130, Appendix III, and described in Section (A)(4) of this part.

Protection of Systems (A) (continued)

Systems Requiring Protection (3) (continued)

Other Applications (d)

This includes all applications not covered under (a) through (c) of this section. Adequate security for these systems is substantially provided by the security of the general support systems in which they operate.

System Protection Requirements (4)

Security Controls (a)

The following four security controls are required to be implemented by OMB Circular A-130, Appendix III, for each NRC General Support System or Major Application. The first two also apply to non-major application systems that are used to process, transmit, or store sensitive unclassified, safeguards, or classified information. (See Exhibit 1 of this handbook.)

- Assigning responsibility for security to a management official knowledgeable in the nature of the information and process supported by the application and in the management, personnel, operational, and technical controls used to support it. (i)
- Planning for the adequate security of each system (This planning process and the SSP developed should address such items as rules of the system, training, personnel controls, incident response capability, continuity of support or contingency planning, technical security, system interconnection, and Privacy Act security requirements). (ii)
- Performing an independent review or audit of the system security controls at least every 3 years to identify possible deficiencies (The security of a system will degrade over time, as technology evolves and as people and procedures change. The review should ensure that management, operational, personnel, and technical controls are functioning effectively.) (iii)
- Authorizing, in writing, a system to process information (This authorization, granted by a management official, provides an important quality control. By authorizing processing in a system, a manager accepts the risks associated with it. Management authorization is based upon an assessment of management, operational, and technical controls performed in the previous step.) (iv)

Protection of Systems (A) (continued)

System Protection Requirements (4) (continued)

Specific Guidance (b)

Sections B through I of this part provide specific guidance for implementing system security requirements. The applicability of these requirements by type of system is as follows:

General Support Systems (i)

- Assignment of a system security officer (SSO) by the system sponsor (*a*)
- Completion of a risk assessment (*b*)
- Preparation of a system security plan (*c*)
- Development and testing of a contingency plan for the system (*d*)
- Performance of a management review of security controls (certification) (*e*)
- Official authorization to process by an NRC management official (accreditation) (*f*)

Major Applications (ii)

- Assignment of a System Security Officer by the system sponsor (*a*)
- Completion of a risk assessment (*b*)
- Preparation of a system security plan (*c*)
- Development and testing of a contingency plan for the application (d)
- Performance of a management review of security controls (certification) (*e*)
- Official authorization to process by an NRC management official (accreditation) (*f*)

Protection of Systems (A) (continued)

System Protection Requirements (4) (continued)

Non-Major Applications Systems That Process Sensitive Data, SGI, or Classified Data) (iii)

- Assignment of an SSO by the system sponsor (*a*)
- Preparation of an SSP (*b*)

Other Applications (iv)

The security of NRC application systems not covered above shall be addressed through the security of the systems on which they operate. For example, LAN, WAN, and data center security controls must provide adequate security for applications in this category. There is no requirement for individual applications in this category to have a separate SSO, security plan, contingency plan, risk assessment, management review of controls, or processing authorization. Rather, these requirements will be addressed as part of the security of the general support system on which the application resides.

User Responsibilities (B)

AIS security is the responsibility of all NRC staff and NRC contractor personnel, and it is especially important to the users of AIS, the SSO, the office information technology (IT) coordinator, the Chief Information Officer (CIO), and computer security staff (CSS), Planning and Resource Management Division (PRMO), OCIO. (See the Glossary of this handbook for definitions of these terms.) (1)

Each user must be aware of his or her responsibilities for the use, protection, and release of information, as described in this handbook. In addition, those who use, operate, or supervise the use or operation of an AIS or AIS facility need to be aware of additional security concerns. Some of these basic concerns include the loss of data, threats, computer crimes, computer viruses, and abuse or unauthorized use of equipment and software. Following are simple precautions for all users of AIS (e.g., workstations, microcomputers, and LANs). (2)

- **Protect Sensitive Unclassified Information**. Sensitive and mission-critical information requires protection from disclosure, alteration, and loss. If it can be avoided, do not store sensitive unclassified data on the internal (hard) drive of a system. As an alternative, store sensitive unclassified data on diskettes, and safeguard diskettes in a closed or locked drawer when not in use. (a)

User Responsibilities (B) (continued)

- **Protect Classified and Unclassified SGI Data**. Only process classified and SGI data with prior approval and authorization. Never process classified and SGI data on a LAN, system connected to a LAN, or workstation with an internal fixed disk. Unclassified SGI may be transmitted over a network if the file is encrypted or if password protected using the WordPerfect enhanced password protection feature (see NUREG/BR-0168, Rev. 1). (b)

- **Protect Individual Unattended Workstation**. Always log off workstations and turn off systems at the end of the work day, log off workstations or lock the keyboard when away from your work station, implement the screen saver password option with the time-out set at no more than 15 minutes, and, when available, use the built-in system password feature that allows the workstation to boot only after the user enters his or her password. (c)

- **Protect Against Viruses**. Never bring unauthorized or personal software to work. Beware of downloaded, borrowed or unsolicited software; these may contain a computer virus designed to capture, alter, or destroy data. Always check a newly acquired file, diskette or downloaded file for viruses before using. (d)

- **Protect Individual Equipment**. Practice good housekeeping at all times, including no drinking or eating around the personal computer, terminal, or workstation. Keep electrical appliances (e.g., radios) away from the computer and data storage media such as tape reels or diskettes. (e)

- **Protect Individual Area**. Recognize, politely challenge, and assist people who do not belong in the area. (f)

- **Protect Individual Passwords**. Use only permitted passwords, change them frequently, use meaningless character strings, safeguard and do not share your individual password with anyone. (g)

- **Protect Individual Files**. Establish and periodically review access privileges for each sensitive file. Inspect individual data to ensure that someone has not tampered with it. (h)

- **Protect Individual Media**. Label and store in an approved security container all diskettes and removable media that contains classified data or SGI (i)

User Responsibilities (B) (continued)

- **Protect Against Disaster.** Back up individual data and files at frequent intervals. Always have backup programs, data, and databases ready to go. (j)
- **Protect NRC Resources.** Use NRC computer resources and email for official business only. Use the Internet for work or mission-related activity only. (k)
- **Protect NRC Network Access.** Use the approved method to dial into NRC systems when working from a remote location. Do not have a modem connected to your NRC workstation and do not dial into a modem connected to any NRC workstation. (l)

Employees have a responsibility to assess the sensitivity of their data and to ensure its security. Ultimately, computer security is the user's responsibility. The user must be alert to possible breaches in security and adhere to the security regulations that have been established within the NRC. The security precautions in this section are not all inclusive, but rather are designed to remind the user and raise his or her awareness toward securing information resources. (3)

System Security Officer (C)

An SSO shall be appointed for each NRC general support system or major application and each system used to process, transmit, or store sensitive unclassified, safeguards, or classified information. The system sponsor shall appoint in writing an SSO for each system under his or her individual control. The SSO should be an individual knowledgeable in the nature of the information and the process supported by the system and in the management, personnel, operational, and technical controls used to protect it. OCIO shall be notified in writing of the assignment of all SSOs. (1)

It is acceptable for one SSO to be responsible for more than one system. It also is acceptable that the system manager be appointed as SSO for the system provided that system manager duties are not performed by a contractor. (2)

The SSO should have a clearance and background investigation appropriate for the highest security level of information processed by the system. The SSO is responsible for implementing the requirements of this handbook and any other system-specific requirements he or she deems appropriate. The SSO shall—(3)

System Security Officer (C) (continued)

- Develop system rules of behavior. (a)
- Implement system security controls. (b)
- Initiate the system certification process. (c)
- Examine and test software for security controls and vulnerabilities. (d)
- Respond to recommendations from the accrediting official. (e)
- Educate users on best security practices. (f)
- Perform review and auditing functions. (g)
- Respond to, investigate, and report security incidents. (h)

Information Classification and Sensitivity Level (D)

Besides general support systems and major applications, some NRC systems may need special protection because of the sensitivity of data used by the system. An agencywide survey will be initiated periodically by OCIO to identify all new AIS that are planned or that have been developed and implemented and that process sensitive data (as defined in the Glossary of Volume 12 of the MDS), SGI, or classified information. The system sponsor should identify new systems and complete the survey form, which will be used by CSS, PRMD, to determine the level of data to be processed on the AIS. (1)

Any changes to a previously defined sensitive, SGI, or classified system, such as physical location of the hardware, transfer of the system to a different hardware environment, modification of the system software, changing of the SSO, or new security control procedures must be reported to the OCIO as amendments to the SSP. NRC information processed by an AIS will be categorized as one of the four following types: (2)

- **Nonsensitive Unclassified Information** (a)

  This category includes information that is not classified, is not SGI or sensitive, and is not defined in the Glossary of Volume 12 of the MDS.

Information Classification and Sensitivity Level (D) (continued)

- **Sensitive Unclassified Information** (b)

  This information 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 information. This term includes Proprietary information, unclassified SGI, naval nuclear propulsion information, and other information withheld from public dissemination under the Freedom of Information Act, and the Privacy Act, the Atomic Energy Act of 1945, as amended (AEA). It also includes information not exported to foreign countries and sensitive unpublished and otherwise unavailable fuel cycle information relating to the technology of enrichment or reprocessing. Sensitive unclassified information is further defined in Volume 12 Glossary of the MDS. Sensitive unclassified information stored, processed, or produced on an AIS, the loss of which could adversely affect the national security interest, shall be protected in proportion to the threat of exploitation and the associated potential damage to national security.

- **Unclassified Safeguards Information** (c)

  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 must be protected pursuant to Section 147 of AEA. This information must be safeguarded against disclosure through restrictions on its storage, processing, or production on protected systems only. Examples of protected systems can be found in MD 12.4, Handbook Part II(F), "Protection of Sensitive Unclassified Information." SGI, with the exception of those systems located in an NRC sensitive compartmented information facility (SCIF) or another DFS-approved facility, may only be stored, processed, or produced on an AIS that is a stand-alone unit with a removable storage medium that is secured in an approved security container when not in use and is not physically or logically connected to any network.

Information Classification and Sensitivity Level (D) (continued)

- **Classified Information** (d)

  Information designated as a "National Security Information," "Restricted Data," or "Formerly Restricted Data," is classified information. With the exception of those systems located in an NRC SCIF or another DFS-approved facility, this information may only be stored, processed, or produced on an AIS that is a stand-alone unit, not physically or logically connected to any network, and has a removable storage medium that is secured in an approved security container when not in use. Classified information may only be transmitted using a system that is considered protected. Examples of protected systems can be found in MD 12.4, Handbook Part II(F).

Risk Assessment (E)

OMB Circular A-130, Appendix III, re-issued in 1996, no longer requires the preparation of a formal risk analyses. It does, however, require an assessment of risk as part of a risk-based approach to determining adequate, cost-effective security for a system. Risk assessment and risk management are crucial elements of the security planning process. NRC uses a risk-based approach to determining system security requirements to ensure that security is commensurate with the risk and magnitude of harm that can result from the loss, misuse, or unauthorized access to, or modification of, system information. Risk assessment includes—(1)

- Identification of information and other assets of the system (a)
- Valuation of the system and associated assets (b)
- Identification of threats that could affect the confidentiality, integrity, or availability of the system (c)
- Identification of potential system vulnerabilities (d)
- Estimation of potential impacts from threat activity (e)
- Identification of protection requirements to control risks (f)
- Selection of appropriate security measures for implementation based upon their cost and benefits (g)

Risk Assessment (E) (continued)

Each system sponsor shall assess risks associated with the operation of each NRC general support system (e.g., minicomputer, mainframe, LAN, WAN) or major application and complete risk assessments under any of the following conditions: (2)

- Periodically, at least every 3 years (a)
- Upon significant change to the system (e.g., software or hardware upgrade) (b)
- Upon discovery of a security breach (c)
- When increases in potential threats to the system are detected (d)
- Upon development of a new system or application (e)

CSS or contractors may be used to provide assistance to the system sponsor or SSO in the performance of a risk assessment. Once the risk assessment has been completed, and the results are documented, OCIO reviews the risk assessment and makes recommendations to the appropriate SSO and system management. The risk assessment process is the first step in the certification and accreditation process. (3)

Depending on the type of AIS and the type of data being processed, the risk assessment methodology used may range from an informal approach requiring minimal resources to a complex process requiring a significant level of effort. The system sponsor should contact CSS to obtain guidance on performing risk assessments on the following types of systems: (4)

- **General Support Systems.** Before implementation of new systems in this category, the system sponsor will conduct a risk assessment using a formal, qualitative or quantitative risk assessment methodology. The system sponsor will coordinate with CSS to obtain further information about conducting the risk assessment. For operational systems in this category, the system sponsor will initiate and perform the risk assessment with assistance from the CSS using a facilitated risk assessment methodology. (a)

Risk Assessment (E) (continued)

- **Major Applications.** A facilitated risk assessment methodology will be used whenever a risk assessment is required for a system classified as a major application. This is true for systems under development as well as operational systems. The risk assessment will be initiated by the system sponsor with the assistance of CSS. (b)

- **Non-Major Applications That Process Sensitive, Safeguards, or Classified Data.** While not required by OMB Circular A-130, the system sponsor may elect to perform a risk assessment and may use a printed questionnaire or an automated software tool to perform an informal risk assessment for each system under control. (c)

- **Other Applications.** The system sponsor will ensure that risks associated with his or her system(s) are assessed as part of the risk assessment conducted for the general support system on which these systems reside (i.e., LANs, WANs, or other computer systems). The system sponsor will coordinate with general support system managers to ensure that his or her application systems are included in the general support system risk assessment. (d)

When NRC applications reside on external mainframe systems accessed through timesharing services at remote AIS facilities, system sponsors conducting a risk assessment should take all necessary actions to ensure that the physical safeguards and the operating system safeguards provide protection and security at an acceptable level. (5)

The system sponsor, in coordination with the CSS, should review the results of the risk assessment to determine the level of safeguards appropriate for these systems. The system sponsor should conduct a cost-benefit analysis as a basis for safeguard selection, risk mitigation, and acceptance of any residual risks. System sponsors are responsible for implementing cost-effective measures consistent with the level of system risk. (6)

System Security Plan (SSP) (F)

An SSP will be developed for each NRC General Support System, Major Application, and each system used to process, transmit, or store sensitive unclassified, safeguards, or classified information as defined in Section (A) of this part. For systems under development, the system sponsor will ensure the SSP is developed early in the system's life cycle

System Security Plan (SSP) (F) (continued)

in accordance with NRC MD 2.5, "Application Systems Life Cycle Management." For systems that already have been implemented, the system sponsor will ensure that the SSP is developed or updated as appropriate. The SSP will be used as an instrument for reducing the risk and magnitude of harm that could result from the loss, misuse, or unauthorized access to or modification of information. The plan provides a basic overview of the security and privacy requirements of the subject system and the organization's plan for meeting those requirements. The format for the AIS security plan can be found in NUREG/BR-0168. (1)

In accordance with the requirements contained within OMB Circular A-130, Appendix III, specific security controls should be included in the security plan for each General Support System and Major Application. This planning process and the security plan developed should address such items as rules of the system, training, personnel controls, incident response capability, continuity of support or contingency planning, technical security, and system interconnection. (2)

Contingency Plan (G)

Procedures for general support systems and major applications are required that will permit the NRC to continue essential functions if information technology support is interrupted. Contingency plans, also referred to "as business continuity plans" or "continuity of operation plans," for major applications should be coordinated with the backup, contingency, and recovery plans of any general support systems, including networks, used by the application. (1)

Contingency plans must be completed for NRC general support systems and major applications (see Section (A)(3) of this part). For newly developed systems, this should be done as part of the development effort. (2)

Using National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) Publication 87, "Guidelines for Automatic Data Processing (ADP) Contingency Planning," as a guide, each system sponsor will develop, test, implement, and maintain contingency plans for his or her general support systems, major applications, and systems processing SGI, sensitive unclassified, or classified data. (3)

Contingency Plan (G) (continued)

Application system recovery capability levels have been developed as a guide for contingency planning purposes (see Exhibit 2 of this handbook). Depending on the type of application and the degree to which the application must be available, CSS will assist in determining the requirements of the contingency plans. However, as a general rule, plans for all applications will be tested annually and will be appropriately updated to reflect results of testing. Testing should consist alternately of checklist, simulation, and parallel testing on a 3-year recurring cycle. (4)

Contingency planning involves more than planning for a move off site after a disaster destroys a data center. It also must address how to keep an organization's critical infrastructure operating in the event of disruptions, both large and small. This broader perspective of contingency planning is based on the distribution of computer support throughout the NRC organization. The contingency planning process includes—(5)

- Identifying applications requiring contingency plans (i.e., general support systems and major applications) (See Exhibit 1 for the relationship of these to NRC mission-critical and business-essential systems as defined in the Year 2000 program.) (a)

- Identifying the resources that support the critical function(s) (e.g., human, processing capability, computer-based services, data and applications, physical infrastructure, and documents and papers) (b)

- Anticipating potential contingencies or disasters by identifying a likely range of problems or things that can go wrong (c)

- Selecting contingency planning strategies by considering what controls are already in place to prevent and minimize contingencies (This strategy normally consists of three parts: emergency response, recovery, and resumption.) (d)

- Implementing the contingency strategies by making the appropriate preparations (e.g., establishing procedures for backing up files and applications, establishing contracts and agreements, or purchasing equipment), documenting the strategies, and training employees (e)

Contingency Plan (G) (continued)

- Testing the plan periodically and revising the plan (This is critical because initially there may be deficiencies in the plan and in its implementation and subsequently aspects of the plan will become outdated as time passes and as the resources used to support critical functions change.) (f)

Certification (H)

System Certification (1)

Certification is an integral part of the accreditation process and is used to determine if a system meets all Federal and departmental policies, regulations, and standards. It is a formal testing of the security safeguards implemented in the system to determine whether they meet applicable requirements and specifications. It is used to establish the extent to which a particular AIS design and implementation meet a specified set of security standards. The AIS security plan should serve as the baseline for certification testing because it covers the major security elements of a system and provides the necessary information and documentation. The certification process primarily addresses software and hardware security safeguards, but also considers procedural, physical, and personnel security measures employed to enforce AIS security policy. (a)

The sponsoring office will ensure that each AIS designated as a general support system or major application is subject to a periodic review leading to accreditation (no less than every 3 years). This will be done in coordination with CSS, with a copy of the results submitted to CSS. Certification involves the following four steps: (b)

- Identification of security requirements (i)
- Identification of security specifications (ii)
- Testing security controls (iii)
- Documenting test results (iv)

Following the completion of certification testing, the results will be documented in writing. The test results will document the effectiveness of pertinent management, development/acquisition, operational, security awareness and training, and technical controls implemented to protect the system. Written test results will serve as the basis for deciding whether the system should be accredited or reaccredited. (c)

Certification (H) (continued)

Software Certification (2)

Additionally, newly developed or acquired software will be certified before implementation on NRC systems. The Application Development Division, OCIO, will ensure that systems security planning and implementation procedures contained in the OCIO document, "System Development and Life Cycle Management (SDLCM) Methodology," are followed and implemented. These procedures clearly define security requirements and controls to be employed on all systems development and maintenance projects. Software in the following categories will be certified as specified:

- **In-House Developed Software.** In accordance with procedures identified in the SDLCM methodology, and as detailed in MD 2.5, the system sponsor ensures that design reviews and systems tests are performed and that a certification of the results is recorded for newly developed software and for existing software when significant modifications are made. (a)

- **Government-Off-the-Shelf Software.** Government-developed software should be examined to ensure that it does not contain features that might be detrimental to NRC AIS security. System sponsors considering the use of Government-developed software should comply with the SDLCM by conducting or arranging for performance of software design reviews and systems tests. (b)

- **Commercial-Off-the-Shelf Software (COTS).** The SSO will ensure that commercially procured software is examined to ensure that the software does not contain features that might adversely affect the security of implemented NRC systems. Special attention should be paid to security-related portions of the software to ensure that the security features function as specified. The SSO may obtain assistance from CSS in evaluating the COTS products. (c)

Security Specifications (3)

Security controls are essential to the NRC AIS security program. It is essential to the program and required by Federal law and by OMB Circular A-130 that security controls (e.g., assigning responsibility for security, security planning, periodic review of security controls, and management authorization) be included as one of the integral functional requirements of all acquired Federal IT resources and AIS equipment, software, or related services. (a)

Certification (H) (continued)

Security Specifications (3) (continued)

NIST guidelines (Special Publication 800-4 and Internal Report [NISTIR] 4749) should be used when acquiring IT resources. NIST Special Publication 800-4 is a complete guide to Federal procurement and NISTIR 4749 contains sample statements of work for computer security services. (b)

Accreditation (I)

Each system sponsor and SSO must identify, reduce, and control risks applicable to systems for which they are responsible. This is accomplished through system accreditation and reaccreditation. Accreditation is the formal declaration or authorization by the accrediting (management) official who has system responsibility and who has reviewed the results of the certification process that appropriate security controls have been implemented for an AIS and that risks have been mitigated to an acceptable level. The requirement for accreditation applies to the types of NRC systems identified in Section (I)(1) of this part. The CIO has been designated the accrediting authority for general support systems and major applications. All other AIS should be certified by the SSO and accredited by the SSO's supervisor.

Accreditation Authority (1)

The classification/sensitivity of the data processed by an AIS is used to determine the accreditation authority for that system. Identification of the appropriate accreditation authority is determined by the following criteria:

- **General Support Systems and Major Applications**. General support systems and major applications require an independent review or audit of the security controls at least every 3 years. Because of the high risk involved in these AIS, the review should be independent of the system sponsor responsible for the system or application. The results of the certification process will be forwarded to the CIO for accreditation. (a)

- **Other Sensitive Unclassified AIS**. Systems processing or storing sensitive unclassified information shall be certified by the system user using a self-assessment methodology and accredited by sponsor management of the system. (b)

Accreditation (I) (continued)

Accreditation Authority (1) (continued)

- **Systems Processing SGI.** Systems processing or storing SGI data shall be certified by the system user using a self-assessment methodology and accredited by sponsor management of the system. (c)
- **Classified AIS.** Systems processing or storing classified data shall be certified by the user using a self-assessment methodology and accredited by system sponsor management. (d)

Memorandum of Accreditation/Non-Accreditation (2)

For major applications and general support systems, CSS or other initiating authority shall obtain and review the results from the certification process, including a review of the security plan, risk assessment report, and the contingency plan. Upon completion of the review process, CSS or other initiating authority will prepare an accreditation or non-accreditation memorandum declaring that either a satisfactory level of AIS security is present, or if not, indicating that the level of risk either has not been adequately defined or has not been reduced to an acceptable level for AIS operations. CSS will forward the memorandum to the appropriate accreditation authority. An AIS may be granted an interim authority to operate in accordance with Section (I)(5) of this part. (a)

For all other application types, the SSO shall obtain and review the results from the certification process and, if satisfied with the results, request written accreditation from the accreditation authority. Along with the request, the SSO shall provide a copy of his or her appointment, the security plan, risk assessment report, the contingency plan, and results of certification testing. (b)

Accreditation Authority Signature (3)

The accreditation authority signs the accreditation memorandum, thus accrediting the system.

Reaccreditation (4)

Reaccreditation is required at least every 3 years. However, an AIS will require reaccreditation sooner if any of the following occurs:

- Major change in system hardware or software configuration (a)

Accreditation (I) (continued)

Reaccreditation (4) (continued)

- Change in the classification or sensitivity level of data on the system (b)
- Following identification of a major security flaw, violation, or security incident (c)

Interim Authority To Operate (5)

An AIS that cannot meet accreditation requirements may operate only if an interim authority to operate is issued by the accreditation authority. An interim authority to operate is valid for only 1 year and is not a waiver of the requirement for accreditation. The interim authority to operate permits an activity to meet its operational mission requirements while completing the accreditation process.

Accreditation Tracking (6)

It is the responsibility of the NRC sponsoring office to identify to CSS all systems that require accreditation. CSS shall maintain an updated list of all systems that must be accredited and shall appropriately file all documentation on each SGI, sensitive unclassified, or classified system, adhering to requirements for documents specified in MD 12.2, "NRC Classified Information Security Program," or 12.6, "NRC Sensitive Unclassified Information Security Program."

Part II

Automated Information System (AIS) Security Controls

The minimum general controls that should be implemented at the system level to minimize risks to the confidentiality, integrity, and availability of the information processed by NRC AIS are discussed in this part.

Physical Security of AIS Assets (A)

Computer Room and AIS Equipment Room Physical Security Controls (1)

The implementation of the following minimum construction requirements for NRC computer and AIS equipment rooms will reduce the exposure of NRC assets to identified risks. The objective of these requirements is to provide all NRC computer and AIS equipment rooms with a means to screen entrants, deny access to unauthorized personnel, and control the flow of materials in and out of the room. The security measures stipulated in this section apply mainly to primary computer rooms and, to a lesser degree, are applicable to equipment rooms. These requirements will be implemented by the facility sponsor. (a)

Rooms adjacent to NRC computer and AIS equipment rooms shall be free of potential physical and environmental threats. Where practical, computer and equipment rooms shall be surrounded by a hallway to prevent environmental threats from being shared and to facilitate monitoring adjacent areas for unauthorized access attempts. (b)

On the basis of the level of risk, computer and equipment rooms should have an automated keycard system to control access for NRC employees having authorized access to the room. (c)

Physical Security of AIS Assets (A) (continued)

Computer Room and AIS Equipment Room Physical Security Controls (1) (continued)

- The system should record all entries to the room and should be capable of producing printed audit trails. (i)
- The audit trails shall be maintained in either electronic or printed form for at least 2 months. These audit trail records should be marked to indicate the sensitivity level of the system to which they pertain (e.g., proprietary or safeguards information, [SGI]) and require commensurate protection. (ii)

There should be no windows that open to the exterior of the building. If windows already exist, a risk assessment will be conducted to determine the feasibility of closing off the windows. At the very least, windows shall not open to the exterior of the building on ground floor levels, and some type of protection from flying glass, debris, and water should be provided for equipment in rooms with windows on upper floors. (d)

For rooms with lowered ceilings and raised floors, computer and equipment room walls shall extend from true floor to true ceiling. (e)

Computer and equipment room doors should be installed with hinge pins on the inside. (f)

The doors should be of sufficient strength to prevent unauthorized entry. (g)

If a computer or equipment room contains a significant portion of the location's AIS equipment assets and is not staffed 24 hours a day, 7 days a week, an intrusion detection system should be installed in the room. Decisions not to install intrusion detection systems should be supported by risk analyses results showing the detection system not to be cost-effective. The system should (h)

- Detect unauthorized entry attempts, as well as motion or sound within the room (i)
- Be programmed to activate an alarm at a security monitoring center that is staffed 24 hours a day (Provide the security center with a listing of NRC personnel to be contacted in the event the alarm is activated.) (ii)

Physical Security of AIS Assets (A) (continued)

Workstation Physical Security Controls (2)

With the increasing development of the distributed client-server environment, physical security in workstation areas increases proportionately. (a)

Users should log off workstations and turn off systems at the end of the work day, log off workstations or lock the keyboard when away from their work areas, implement the graphical user interface screen saver password option with the time-out set at no more than 15 minutes, and, when available, use the built-in system password feature that allows the workstation to boot only after the user enters his or her password. (b)

Whenever possible, workstation monitors should be positioned to preclude casual viewing of sensitive data during processing. (c)

Users should back up essential data that is stored on workstations on a regular basis. Backups should be stored in a desk drawer or filing cabinet elsewhere in the office area to ensure physical separation of backups from the system. (d)

Printers in office areas should be placed in an area where access can be controlled to ensure that only authorized personnel access sensitive hardcopy output. SGI must not be sent through a local-area network (LAN) server to a printer. (e)

Network Physical Security Controls (3)

NRC facility managers should implement physical security procedures to ensure that the confidentiality, integrity, and availability of NRC networks is sufficient to ensure secured operation. (a)

Requirements for network server console security features should be incorporated into equipment acquisition requirements. (b)

The following controls for network routers, bridges, gateways, and servers shall be implemented to protect the physical security of network assets. (c)

- Place all network equipment in secured computer or equipment rooms. If this is not possible, secure the equipment in locked rooms, such as the telephone or wiring closets. (i)

Physical Security of AIS Assets (A) (continued)

Network Physical Security Controls (3) (continued)

- Keep telephone and wiring closets that house network cabling or equipment locked at all times. Restrict access to the telephone and wiring closets to a limited number of accountable personnel. (ii)
- Keep consoles logged off or locked out when not attended. If the server does not provide for console protection, physically or logically lock keyboards and consoles at all times. (iii)
- Limit access to the computer and AIS equipment rooms where network equipment resides to those personnel who must access the rooms to perform their duties, such as network and system administrators and telecommunications technicians. (iv)

Network physical security safeguards should be integrated into network design configurations and modifications. (d)

Enough redundancy should exist in available telecommunications lines to avoid single points of failure. Decisions not to provide redundancy in telecommunications should be supported by a risk analyses that shows the redundancy not to be cost-effective. (e)

Key and Combination Control Procedures (4)

It is essential for the protection of all NRC assets that the sponsoring office establish, document, implement, and enforce effective key and combination control procedures. (a)

The NRC sponsoring office should create a comprehensive inventory of all keys and combinations related to the security of office areas, systems equipment, and sensitive materials under their control. The inventory should include room number, number of keys, individual(s) issued to, and date issued. The inventory itself should be appropriately (e.g., provided protection at the level of the information being protected by the key or combination) secured. (b)

All individuals should sign for their key(s). Master keys should only be assigned to a select number of personnel. (c)

Physical Security of AIS Assets (A) (continued)

Key and Combination Control Procedures (4) (continued)

Individuals signing for keys should be cautioned not to duplicate the key. (d)

All unassigned keys should be properly secured. (e)

Semiannual inventories of all keys should be conducted and recorded. Maintain the inventories as official records for 1 year after they are no longer current. (f)

Include the Division of Facilities and Security (DFS), Office of Administration, as a control point in agency exit procedures to ensure that individuals departing the agency turn in all assigned keys. (g)

Immediately report lost or stolen keys to DFS. (h)

When individuals no longer have a need for access, ensure that combinations are changed immediately. (i)

DFS should have any lock(s) re-keyed for which the key(s) are missing and issue new keys to authorized personnel. (j)

Environmental Security Controls (B)

The facility sponsoring office should incorporate necessary controls to mitigate environmental threats (e.g., fire, water) to AIS and operations. For many types of computer equipment, strict environmental conditions should be maintained. Manufacturer's specifications should be observed for temperature, humidity, and electrical power requirements. The facility sponsoring office should ensure that appropriate environmental controls are properly installed, implemented, and maintained to protect NRC AIS resources.

Housekeeping (1)

Users should not eat or drink near AIS equipment, and should keep electrical and magnetic items away from such equipment. Spaces within the vicinity of the AIS equipment shall be kept free of dirt, dust, and debris.

Environmental Security Controls (B) (continued)

Fire Protection (2)

A fire detection system provides early warning that smoke and/or fire has been discovered and a response action needs to be taken immediately. Fire protection will normally be supplied by the building fire protection system. Class A and C portable fire extinguishers should be available and located so that an extinguisher is readily available within 50 feet of travel of any part of the facility. A sign should be located adjacent to each portable extinguisher and should plainly indicate the type of fire for which the extinguisher is intended.

Protection From Water Damage (3)

To prevent damage from falling or blowing water, facility sponsors should consider obtaining plastic coverings for all AIS equipment located in computer or equipment rooms. Such coverings should be readily available in the vicinity of computer equipment to allow rapid employment in the event of a water emergency (i.e., sprinkler activation, broken window).

Power Protection (4)

NRC facility sponsors should ensure that all AIS equipment is protected with surge protection, and if warranted because of its criticality, equipment should be supported by an uninterruptible power supply system.

Administrative Security Controls (C)

Individual Use of AIS (1)

AIS are installed to conduct NRC business and are to be used for official agency business only. The use of AIS capabilities for personal use is prohibited. Similarly, users may not use personally owned AIS to perform NRC-related work without advanced approval of their supervisor, preferably in writing.

Management of User Identifications and Passwords (2)

This section applies to those AIS in which user identification codes (user identifications [IDs]) and passwords are a function supported by the AIS operating system. It is recognized that an AIS operating system may not support this capability, in whole or in part. For example, an AIS operating system may support passwords, but can only support a password length of less than or equal to five characters. (a)

Administrative Security Controls (C) (continued)

Management of User Identifications and Passwords (2) (continued)

When available, user IDs and passwords are required to be used for entry into AIS that process, store, or transmit SGI, sensitive unclassified, and classified information. Those users who have microcomputers or workstations that have password capabilities for logging on should implement the feature that allows the computer to boot only after the user enters a password. In addition, if the keyboard lock capability exists, such as in the NT operating system environment, it should be implemented as well. This lock will safeguard the system against unauthorized use when the user must be absent from the machine. Systems administered by others (e.g., the National Institutes of Health [NIH]) are excluded; however, users of those systems are required to follow the user ID and password guidance required by the host entities. Rules and guidelines are set to protect NRC AIS from destruction, modification, unauthorized usage, denial of service, and unauthorized disclosure of NRC data or information by unauthorized users. (b)

The Office of the Chief Information Officer (OCIO) assigns IDs and passwords through various system support staff. The Information Technology Infrastructure Division, OCIO, will coordinate the issuance of computer security identification (IDs and passwords) for LANs and wide-area networks (WANs), intelligent gateways, and other agency external access routes specified in this handbook. High-performance computer system supervisors authorize accounts on the advanced computer system(s) using OCIO-assigned IDs. Address any questions about system access to the OCIO Customer Support Center (415-1234). (c)

For AIS that require a user ID and a password, the following rules should be observed: (d)

- User IDs and passwords should not be shared or written down. (i)
- Passwords should be changed at least every 90 days. (ii)
- If a password has been seen or guessed by another, it should be changed immediately. (iii)
- Passwords should be at least six characters in length. (iv)
- Passwords should not be an English word, name, or string of characters easily guessed, for example, your birthday or telephone number. (v)

Administrative Security Controls (C) (continued)

Management of User Identifications and Passwords (2) (continued)

- If the feature is available, when logging onto an AIS, the user should be given a limited number of chances to enter the correct user ID and password. After the maximum number of incorrect attempts, the system will lock the user out until the situation is reported to the SSO or the system administrator (for large systems). This action prevents outsiders from attacking the AIS by using a known user ID and trying to guess the password. (vi)

Telecommuting, Flexible Workplace, and Remote Access (3)

NRC employees are authorized to take non-sensitive material home to work on if the worker has his or her supervisor's permission. Participants in the NRC Flexible Workplace Program must agree to the security provisions listed in the Attachment to and sign NRC Form 624, "USNRC Flexible Workplace Program Participation Agreement." Personnel are not permitted to take classified or SGI work home under any circumstances. Security provided NRC information resources should be equivalent to that provided in the office environment. NRC managers and system security officers (SSOs) should encourage workers to back up their work regularly, not to share data with persons who are not authorized to access the data or who do not have a need to access the data to perform their job, and to consider the increased potential for virus infection of diskettes when used outside the workplace. Virus scanning software will be installed on all systems used to remotely access NRC systems, and will be provided to users for home use upon request to the Computer Security and Oversight Office. NRC managers should ensure that users comply with all copyright laws and that software packages are used at home only when authorized by license. Dial-in users are of special concern to security personnel and system administrators. Additional security considerations are discussed in Section (E) of this part and should be implemented before starting a dial-in activity.

Security of Portable Computers (4)

Because of their portability, security risks to sensitive data on laptop computers are greater than for stationary systems. Users of such systems should comply with the requirements of Management Directive (MD) 13.1, "Property Management," to ensure that sensitive data residing on portable computers is protected against loss, disclosure, destruction, or modification. No classified information or

Administrative Security Controls (C) (continued)

Security of Portable Computers (4) (continued)

SGI is to be accessed, processed, stored, or telecommunicated and no sensitive unclassified information is to be telecommunicated.

Electronic Mail (5)

All NRC AIS, including the software and information stored and created on these systems are property of the Government and considered "for official use only." NRC managers should ensure that system users are aware that they should have no expectation of privacy when using NRC electronic mail (email) systems. They should be informed that just as with any system information and data, email messages are subject to be read and audited by systems management and/or security personnel.

Reporting Incidents and System Anomalies (6)

The most important consideration in responding to security-related events is establishment of an effective means of immediately reporting incidents to authorities who are responsible for their investigation (i.e., the Customer Support Center for system anomalies; the Computer Security Staff (CSS), OCIO, for AIS-related incidents; the DFS for physical security breaches; and, law enforcement authorities for criminal violations). For each sensitive unclassified system, the SSO should establish procedures for system users to immediately report computer incidents to the SSO, and for the SSO to pass along this report to the appropriate investigating authority. These procedures should include:

- A description of what should be reported (a)
- An identification of who the incident should be reported to (b)
- Information to be obtained, such as a description of the incident, date and time of the incident, the significance of the incident, personnel involved, and corrective actions taken (c)

Investigating Incidents (7)

Upon notification by users, managers, or the CSS, sponsoring office management with the assistance of the SSO should take immediate action to investigate security incidents. The SSO should attempt to determine the cause and significance of the event and should seek to

Administrative Security Controls (C) (continued)

Investigating Incidents (7) (continued)

limit damage as quickly as possible. CSS should be notified of all incidents that place networked systems potentially at risk. Once reported, the SSO should coordinate with CSS to determine corrective actions necessary to preclude recurrence of the incident.

Warning Banner (8)

NRC managers should ensure that all users are aware of their responsibilities for proper use of the system and the prohibitions against misuse of the system and that their activities on the system are subject to monitoring. (a)

Systems shall be configured to display the following warning banner to users upon first accessing NRC automated information resources: (b)

USE OF THIS COMPUTER CONSTITUTES A CONSENT TO MONITORING.

This computer system is for official or authorized use only. Federal computer systems are subject to monitoring for maintenance, to preserve system integrity and security, and for other official purposes. You should not expect privacy, nor protection of privileged communication with your personal attorney, regarding information you create, send, receive, use, or store on this system.

If monitoring reveals possible evidence of violation of criminal statutes, this evidence and any related information, including your identification, may be provided to law enforcement officials, including the Office of the Inspector General. Anyone who violates security regulations or makes unauthorized use of Federal computer systems is subject to criminal prosecution and/or disciplinary action.

UNAUTHORIZED ACCESS PROHIBITED BY LAW — TITLE 18 U.S. CODE SECTION 1030.

Public Law 99-474 provides that anyone who accesses a Federal computer system with or without authorization, and by means of such conduct obtains, alters, damages, destroys, or discloses information, or prevents authorized use of information on the computer, shall be subject to fine or imprisonment, or both.

Administrative Security Controls (C) (continued)

Inventory of Applications (9)

System managers should know the sensitivity level and type of data users have on NRC systems for which they are responsible. CSS shall conduct, with the assistance of systems sponsors, a periodic NRC officewide survey to identify all general support systems, major application, and other systems that are used to process, transmit, or store sensitive unclassified, safeguards, or classified information.

Asset Inventory (10)

To ensure that NRC AIS resources are properly controlled and accounted for, system sponsors should conduct an inventory of all system hardware and software annually. This should be a visual inspection of all hardware devices, and a random check of software residing on system workstations. This inventory should be conducted using reports generated from configuration management databases described in Section (C)(11) of this part..

Configuration Management (11)

Each system sponsor should create a database to record pertinent AIS hardware and software information. This includes file servers, networking assets, laptops, workstations, and printers as well as commercial and Government-developed software programs and packages. At a minimum, the following information should be captured:

- Person overall responsible for equipment and/or software, such as the name of the supervisor of the user of the equipment, or the name of the user of the software (a)
- Organization, such as the office code of the person responsible for the equipment or software (b)
- Location of the equipment or software (i.e., office or room number where it is physically located) (c)
- Nomenclature of the equipment or software (d)
- Serial number of the equipment (e)
- Version number and serial number of the software (f)
- Licensing and warranty information, if any, for the software (g)

Administrative Security Controls (C) (continued)

Visitor Control (12)

To safeguard sensitive data from disclosure to unauthorized or uncleared personnel, the NRC managers should ensure that procedures for controlling visitors are established and enforced. Visitors should not be allowed into areas where sensitive, safeguards, or classified data is being processed, stored, or transmitted unless accompanied by an escort. NRC personnel who are responsible for escorting visitors should be made aware of the importance of their duties. A means of recording visitors' entries and exits should be implemented for either the facility or the specific area where sensitive information is processed or stored. System users should be instructed to challenge persons they do not recognize.

Virus Controls (13)

All NRC AIS should have virus detection software installed and set up to scan all local drives at system boot. Additional protection of scanning all diskettes every time they are inserted into a drive may be desirable for AIS that are particularly susceptible to viruses. All diskettes and CD-ROM disks should be scanned with approved virus detection software before being inserted into the disk drive of an NRC system. Scanning of diskettes should be performed on a stand-alone system so as not to infect network systems. Any files that are downloaded from any open access system (including Bulletin Board Systems, the Internet, or online services) should be scanned from a diskette. Files that are in compressed format should be extracted before scanning for malicious software. If a virus is detected, the SSO, system administrator, and CSS should be notified immediately. Personnel should attempt to eradicate the virus with antivirus software while attempting to isolate it to a single system and/or media.

Personnel Security Controls (D)

Personnel security generally refers to a program that determines the sensitivity of positions and screens individuals who participate in the design, operation, or maintenance of AIS or who have access to such systems. Personnel security is part of the set of security controls designed to ensure the confidentiality, integrity and availability of NRC AIS.

Personnel Security Controls (D) (continued)

Personnel Security Principles (1)

For the purposes of this discussion, personnel security is a means of screening individuals and granting access rights to NRC AIS only to those individuals with a verifiable need for access who also meet the security requirements for a position. Positions should be categorized according to the sensitivity of the information processed and should be reviewed annually to ensure appropriate security requirements are in place. All NRC personnel who will be involved in the processing of sensitive unclassified, safeguards, or classified information should have the appropriate level of clearance before being granted access to such systems.

Position Definition (2)

System sponsors should identify and address security issues early in the process of defining a position. Once a position has been broadly defined, system sponsors should determine the type of computer access needed for the position. System sponsors should consider the following two general personnel security principles when determining access: (a)

- **Separation of Duties.** Roles and responsibilities should be divided so that a single individual cannot subvert a critical process. (i)
- **Least Privilege.** Users should be granted only those accesses required to perform their duties. Least privilege may mean that some employees have significant access if required for their position. However, application of this principle may limit the damage resulting from accidents, errors, or unauthorized use of system resources. (ii)

A supervisor should carefully determine the duties, responsibilities, and access levels in accordance with these principles before actually staffing a position. Knowledge of the duties and access levels that a particular position will require is necessary for determining the sensitivity of the position. (b)

Personnel Screening (3)

Background screening determines whether a particular individual is suited to occupy a given position. In positions requiring a high degree of trust, the screening process should attempt to document the person's trustworthiness and the appropriateness of holding a particular

Personnel Security Controls (D) (continued)

Personnel Screening (3) (continued)

position. Personnel, including contractors, selected for IT-I and IT-II positions, as described in MD 12.3, "NRC Personnel Security Program," Handbook Part I, will undergo personnel background screening. The personnel security screening requirements of MD 12.3 do not apply to work let to DOE under the requirements of MD 11.7, "NRC Procedures for Placement and Monitoring Work With the U.S. Department of Energy (DOE)."

Termination of Access Rights (4)

Each system sponsor should establish AIS access rights termination procedures for departing personnel, staff and contractors, whether for voluntary or involuntary termination. Also, it may be necessary to suspend access to individuals who are temporarily absent from their place of work for periods longer than 90 days. This requirement should be addressed on a case-by-case basis with a final determination made by the system sponsor. At a minimum, these procedures should include the following: (a)

- Removal of access permissions to critical or sensitive areas, such as telephone closets (i)
- Removal of access permissions to all systems from mainframes to desktops as well as internetworking systems such as LAN (ii)
- Expiration or removal of user IDs (If the user's ID and password are shared by others, the password should be changed immediately.) (iii)
- Expiration or removal of external communications log in ID assigned to the user (iv)
- Retrieval of NRC-owned hardware, software, and documentation (This includes employees signing a statement that they will remove any software purchased by NRC from their personal computer (PC) at home.) (v)
- Retrieval of any NRC AIS-related information, documentation, or manuals in an employee's possession (vi)
- Requirements for reporting employee terminations and temporary absences to the SSO and CSS (vii)

Personnel Security Controls (D) (continued)

Termination of Access Rights (4) (continued)

System sponsors should ensure that NRC users are aware of their responsibility to report unauthorized use or abuse of NRC AIS facilities and equipment. Additionally, all NRC AIS users should be aware of fellow users' behavior and report the potential for AIS abuse (e.g., by a disgruntled employee) to supervisory and AIS security personnel (e.g., SSO). (b)

Nondisclosure of Information (5)

NRC managers and security personnel, to include SSOs and CSS, should take precautions to ensure that NRC personnel and contractors having access to sensitive, safeguards, or classified information are aware of their responsibility and legal obligation to safeguard these types of information when processed, stored, or transmitted on NRC AIS.

System Security Controls (E)

General (1)

System-level technical control measures (identification and authentication, discretionary access, auditing, system integrity, data integrity, reliability of service, and password controls) described in this section are not intended to be system specific, but rather, to provide a policy level template that the system sponsor, SSO, and the system manager or administrator should implement as applicable to any specific system or application. Specific security parameters for Novell NetWare, Windows NT, and UNIX NetWare systems are provided in Exhibits 3, 4, and 5, respectively, of this handbook. (a)

The technical controls of the systems should be implemented as described whenever supported by the hardware and software of the system. If the feature is not supported, it should be considered as a possible inclusion in future upgrades if economically feasible. All new system development and acquisition should include these controls as part of the design specifications. Efforts should be made, when using commercial of-the-shelf (COTS) software products, to identify and procure those which support these controls. Individual custodians of information that require a higher level of protection than that afforded by system level controls are responsible for coordination with system administrators and/or sponsors to integrate application-specific controls. (b)

System Security Controls (E) (continued)

Identification and Authentication (I&A) Controls (2)

I&A controls provide the capability to establish, maintain, and protect a unique identifier and password for each authorized user. It also provides the capability to establish, maintain, and protect from unauthorized access, information that can be used to authenticate the association of a user with that identifier. I&A protects against attempts by unauthorized users to gain access to the system. I&A mechanisms also prevent authorized system users from accessing resources to which they have not been authorized. (a)

General I&A controls include the following actions: (b)

- Ensure that all default system accounts (e.g., "admin", "guest") and passwords (e.g., "guest", "test", "system") are deleted or disabled before implementation of any new system. This pertains to both hardware and software systems to include operating systems, servers, and routers. (i)
- Assign unique user IDs to identify users to the system. (ii)
- Require users to identify themselves with their user IDs before being allowed to access any AIS resource. (iii)
- Ensure that all processes running on behalf of the user shall have the user ID of that user associated with it. (iv)
- Enable an administrative privilege that will permit the disabling of specific user IDs. (v)
- Where the system will support the feature, set the system to disable user IDs after 90 days of inactivity. (vi)
- Enable the password mechanism to authenticate the claimed identity of a user. (vii)
- Set the system to perform entire user authentication when an invalid user ID is entered. The error message should simply state that the logon information is invalid, but not specify which part of the information is incorrect. (viii)
- Set the system to end the logon session after three unsuccessful logon attempts. (ix)

System Security Controls (E) (continued)

Specific Password Controls (3)

The implementation and enforcement of proper password standards are essential to protecting the system and application components of NRC resources from unauthorized access. Where individual systems will support them, systems should be set to enforce the following standards:

- The system should accept only passwords that are a minimum of six characters and are **a combination of alphabetic and numeric characters** (or special characters such as $, #, @). (a)
- The system should automatically force all users to change passwords a minimum of every 90 days. Set the system to automatically lock out a user who violates this procedure and to ensure the new password is different than the old password by at least two characters. (b)
- Set the system to suppress any appearance of passwords on the screen. (c)
- All passwords should be stored in a one-way encrypted form. This feature should be supported by system components such as the network operating system, workstations operating systems, and application security systems. (d)
- Limit access to the encrypted passwords to system, network, and application security administrators as applicable. (e)
- Audit all changes to password files. (f)

User-Defined Password Standard (4)

Where passwords are manually generated by users, they should be instructed to ensure that the following guidelines are followed:

- Passwords should consist of a minimum of six alphanumeric characters and be **a combination of alphabetic and numeric characters** (or special characters such as $, #, @). (a)
- Passwords should be changed a minimum of every 90 days, or whenever the integrity of the password is suspected to have been compromised. (b)
- New passwords should be different from old passwords by at least two characters. (c)

System Security Controls (E) (continued)

User-Defined Password Standard (4) (continued)

- Passwords such as the birth date or name of a family member or sequential letters of the alphabet should not be chosen. These may be easily guessed by unauthorized users. (d)
- The use of English or foreign language words as passwords should be avoided. Words may be "guessed" by dictionary programs run during remote access by unauthorized users. (e)
- Passwords should never be written down. (f)
- Passwords should not be stored online or in a file on workstations or on diskettes. (g)
- Passwords should never be shared with others, including coworkers. (h)
- Each user should be assigned their own unique user ID. User IDs and "guest" accounts should not be shared among multiple users. (i)

Discretionary Access Controls (5)

Discretionary access controls allow the administrator to configure the system to ensure that authenticated users can access and perform operations on only the system resources for which they have authorization. The resources include directories, files, applications, LAN, WAN, and database management systems. The operations include, but may not be limited to, read, write, execute, delete, modify.

- Set the system to grant access to system resources only after the user is properly authenticated. (a)
- Ensure that only administrators have the authority for the creation, deletion, or modification of user access authorization data. (b)
- Set the system to automatically terminate a user session after three attempts to access restricted resources. (c)
- Establish permission controls to designate which users and groups are granted which specific access permissions. Access permissions should be modified only by the sponsor or system administrator. (d)

System Security Controls (E) (continued)

Auditing Controls (6)

Auditing controls support accountability by providing a trail of user actions. These actions are associated with individual users for all security-relevant events and are stored in an audit trail. The audit trail can be examined to determine what happened and what user was the instigator of the security-relevant event. The SSO should review audit reports or audit trails on a daily basis. The audit trail data should be protected from unauthorized access, modification, or destruction using the following controls:

- Configure audit trail features to provide user accountability for security administration actions. (a)
- Ensure that audit files are accessible to only those individuals who require access to them. (b)
- Where the system will support it and the performance of the system can be maintained at an acceptable level, record the following events in the audit trail: (c)
  - User logons, both successful and failed (i)
  - Unsuccessful attempts to access objects (resources) or perform functions that are denied by lack of privileges or rights (ii)
  - Successful accesses to security-critical objects (i.e., operating system files, data with high sensitivity) (iii)
  - Changes to users' security privileges/profiles (iv)
  - Changes to the system security configuration (v)
  - Modification of system-supplied software (vi)
  - Creation and deletion of objects (vii)
  - Organization defined or application specific events (viii)
  - Activities of a specified user ID (ix)

System Security Controls (E) (continued)

Auditing Controls (6) (continued)

- Where possible and applicable, for each audited event, record the following information in the audit record: (d)
  - Date and time of the event (i)
  - User ID and associated point of physical access (node, port, network address, or communication device) (ii)
  - Type of event (iii)
  - Names of resources accessed (iv)
  - Success or failure of the event (v)
- Where possible, automate the parsing of audit trails into audit reports that contain the minimum events necessary to identify suspicious or unauthorized activity. (e)

System Integrity Controls (7)

System integrity controls promote separation of user and system processes and data; protect software, firmware, and hardware from unauthorized modifications (deliberate and accidental); and control user and maintenance personnel actions. System sponsors should take action to ensure that the following controls are implemented on their systems to the greatest extent possible:

- Separate and protect user processes and their data from other user processes. System programs should be separated and protected from any user processes. (a)
- Review modification dates, check sums, and digital signature features as part of the auditing process to verify the integrity of delivered software. (b)
- Set the system to restrict the use of privileged instructions to the minimum necessary amount of administrators. (c)
- Configure the system to ensure that the execution of system maintenance or repair software, modification, or replacement of system and application software requires administrator privilege. (d)

System Security Controls (E) (continued)

Data Integrity Controls (8)

Data integrity mechanisms ensure that data is entered and maintained in a correct and consistent state. The following requirements provide for controls that promote tracking of changes to resources and protect data against exposure, unauthorized modification, or deletion while it is stored or transmitted over a network:

- Configure applications and systems to audit the time and date of the last modification to resources, as well as the identity of the user who performed the modification or transaction. (a)
- Where determined to be appropriate by the risk analyses process, and if technically feasible and cost-effective, employ encryption controls to preserve and verify the integrity of stored or transmitted data. (b)

Reliability of Service Controls (9)

The following reliability of service requirements ensure continuous accessibility and availability of system resources to authorized users. These requirements also prevent or limit interference with time-critical operations and allow the system to maintain an expected level of service during adverse (deliberate or accidental) conditions.

- Configure the system to detect and report all conditions that degrade service below a specified minimum. (a)
- If practical, configure the system to place limits on the amount of the total disk and central processing unit resources an individual or group can utilize. (b)

Telecommunications Security Controls (F)

General Network Security Guidelines (1)

Controlling access to NRC networks by the Information Technology Infrastructure Division (ITID), OCIO, is an important step in ensuring information is protected. ITID also is responsible for implementing all necessary security measures to protect NRC LANs, WANs, other networks and their services from unauthorized access to; unauthorized modification, destruction, or disclosure of data; and incidental or willful interference of regular operations from insiders, casual hackers,

Telecommunications Security Controls (F) (continued)

General Network Security Guidelines (1) (continued)

or other unauthorized sources. This includes protection of data, login access to hosts and networks, and availability of hosts or networks to perform their critical functions correctly, without harmful side-effects. The ITID is responsible for performing telecommunications security functions specified in MD 12.4, involving the security of systems used to transmit classified, SGI, or sensitive unclassified data to other systems. Implementation of proper safeguards, as listed below, is key to controlling access to NRC network resources and to protecting AIS resources from unauthorized access.

- A primary and alternate administrator should be designated for each NRC LAN and multi-user computer system to perform security functions. The number of personnel granted access privileges equivalent to those of the administrator should be strictly limited. (a)
- The primary user of each workstation or microcomputer connected to an NRC LAN or other network is responsible for the general maintenance and security of the computer and for following all policies and procedures associated with the use of the computer. These users should be trained and given guidance so that they can adequately follow all policies and procedures. (b)
- In order to prevent unauthorized access to NRC data, software, and other network resources, all security mechanisms should be under the exclusive control of the applicable SSO and system administrator. (c)
- All backups of server files and programs should be conducted under the control of the network or system administrator. (d)
- Use of traffic monitors and recorders (e.g., sniffers and traffic analyzers) must be authorized by the CSS. System sponsors may, where appropriate, grant specific individuals or offices approval for the routine and reoccurring use of such equipment and software on their systems. (e)

Telecommunications Security Controls (F) (continued)

General Network Security Guidelines (1) (continued)

- Computer security awareness training is an integral part of the AIS security program. Employees responsible for the management, operations, and use of NRC LANs and other networks should receive training in computer security awareness and acceptable computer practices. (f)
- Audit reduction tools should be implemented to gather search and print audit records from diverse network devices by various parameters such as event type, elapsed time, date, and user ID. These software tools should be capable of parsing raw audit trails to create audit reports that contain only the events necessary to indicate suspicious or unauthorized activity. (g)
- A security violation should generate an alarm to the SSO or system administrator, as well as the system console. (h)
- Audit files should be protected from general access and encrypted when possible. (i)
- Whenever possible, all passwords should be encrypted when transmitted. (j)
- Local procedures for backing up all data and software from network servers shall be fully documented and performed. (k)
- File access controls should be provided at directory, subdirectory, and file levels. (l)
- All licensed software should be stored in designated "execute only" or "read only" directories. (m)
- User accounts should be automatically suspended after 90 days of inactivity and terminated after a year of inactivity. (n)

Dial-Up Security Guidelines (2)

It is essential that sensitive data stored in NRC AIS be protected against modification, destruction, and disclosure. Dial-up access introduces an additional set of vulnerabilities to NRC networks and systems because the typical dial-up communications circuit is linked to the public telephone network. The very nature of dial-up

Telecommunications Security Controls (F) (continued)

Dial-Up Security Guidelines (2) (continued)

communications implies that the user may be anywhere in the world that the telephone network reaches. Anyone who comes into possession of the telephone number for a computer's dial-up port may attempt to gain access. This can make the dial-up path a direct connection from the public network into the agency's network or system bypassing access controls, such as firewalls, designed to protect its borders. The purpose of placing additional access controls on dial-up lines is to perform the job of screening incoming calls to verify that the workstation connection itself is valid.

Dial-In Access Control Features (a)

All direct dial-up access to NRC networks and systems should be afforded an additional layer of logical access control over and above those provided by the operating system of the systems or the applications. Where dial-in service provides potential access to sensitive NRC systems and applications, the following control features should be implemented:

- If a telephone connection through an incoming modem is interrupted, the system should automatically log out the user or require re-authentication before allowing the user to resume the processing. (i)
- Incoming modems should automatically disconnect an incoming call if the caller logs out or if the caller's logon process is terminated. (ii)
- Employ, at a minimum, a modem or communication access server that requires using combinations of a user's unique user ID, password, token, or personal identification number (PIN). In addition, one or more of the following safeguards may be employed to protect dial-in access to highly sensitive systems: (iii)
  - Callback (*a*)
  - Portable challenge-response units (*b*)
  - One-time use password devices (*c*)
- Audit all dial-up access in accordance with guidelines in system security policies and in a manner that would allow identification of dial-up sessions. (iv)

Telecommunications Security Controls (F) (continued)

Dial-Up Security Guidelines (2) (continued)

- If possible and cost-effective, auditing should include caller identification from the public telephone network. Caller ID is often an integral part of modern integrated services digital network [ISDN] dial-in service. (v)
- Physically protect the modems and telephone lines (e.g., locked telephone closets, modem pool rooms). (vi)
- Do not publish modem telephone numbers. Provide modem numbers only to authorized individuals. (vii)
- To maintain centralized and uniform control of dial-in access security controls, all dial-in must be accomplished through connections approved by the Director, ITID. Remote dial-in to individual PCs using remote control access packages, such as PCAnywhere and Reachout, is prohibited. (viii)
- The Director, ITID, should exercise extreme care in authorizing individually managed remote control dial-in service. If approved, these services must conform to the same dial-in controls as specified for all other dial-in service. (ix)
- In addition, any PCs being used to provide individually approved remote control dial-in service, and supporting transmission control protocol and Internet protocol (TCP/IP) , should be configured to be automatically powered off at the end of a call or upon reboot. (x)

Remote Access Agreement (b)

Users granted approval to remotely access NRC systems should be required to read and sign an AUTOS Remote Access Agreement (Exhibit 6 of this handbook). This agreement documents the user's acknowledgment of rules applicable to remote access.

Guidelines for Internet Security (3)

It is essential that sensitive data stored and processed in NRC systems be guarded from modification, destruction, and disclosure. Connection to the Internet means that the general public has potential access to sensitive NRC systems. The access controls augment the existing access controls provided by NRC AIS general support systems and

Telecommunications Security Controls (F) (continued)

Guidelines for Internet Security (3) (continued)

applications to minimize the risk of unauthorized modification, destruction, and disclosure (see item (a) below).

NRC Internet Access Security Requirements (a)

- Classified and SGI data should never be transmitted via the Internet. Sensitive unclassified information should not be transmitted via the Internet unless it has been encrypted using an encryption scheme that has been approved by CSS. NRC sensitive unclassified information should not reside on Internet servers without specific approval from CSS. (i)
- Provide and use an approved (certified) firewall capability to control access to and from the Internet. Firewalls consist of a wide range of devices and architectures that protect networks. The firewall shall be located in the logical path between the NRC intranet (and consequently, the public networks) and internal NRC networks. (ii)
- NRC should maintain firewall capabilities between any NRC sensitive unclassified system and the Internet. (iii)

Minimum Firewall Capabilities and Configuration (b)

The set of requirements listed below are intended to define a set of minimum standards for devices or architectures that provide firewall capabilities to protect sensitive NRC systems and networks from public access. These requirements are intended to be the minimum set of features, but the firewall need not be limited to the features listed.

- The firewall should include, at a minimum, the capability to screen and filter traffic at the transport and network layers of the open systems interconnection (OSI) model. This screening capability should include filtering of the source and destination IP packet addresses and traffic-type filtering on the basis of TCP and user datagram protocol (UDP) port addresses. (i)

Telecommunications Security Controls (F) (continued)

Guidelines for Internet Security (3) (continued)

- If NRC systems are accessed from the Internet, firewalls controlling the access should be capable of analyzing the traffic at all layers of the OSI model, to include the application layer and making it capable of permitting or denying access to specific applications on systems within NRC networks. In addition, all NRC passwords and data transferred via the Internet should be encrypted, using, at a minimum, the triple Data Encryption Standard (DES, see Glossary of this handbook). (ii)
- The firewall should be configured to deny all NRC-internal addresses originating from the Internet side of the firewall. (iii)
- The firewall should be configured to deny all non NRC (external) addresses from originating from the NRC internal side of the firewall. (iv)
- The firewall should be configured to deny any service (TCP or UDP port address) unless it is expressly permitted. (v)
- The firewall should prevent the following traffic types (TCP or UDP ports): (vi)
  - **Trivial file transfer protocol (TFTP, port 69).** TFTP is used for booting diskless workstations, terminal servers, and routers and can also be used to read any file on the system if set up incorrectly. (*a*)
  - **X windows, open windows, ports 6000+, port 2000.** These services can leak information from X window displays including all keystrokes. (*b*)
  - **Remote procedure call (RPC, port 111).** These services include network information service (NIS) and network file system (NFS), which can be used to intercept system information (e.g., passwords) and read and write to files. (*c*)
  - **Remote login, remote shell, and remote execute (rlogin, rsh, and rexec, ports 513, 514, and 512).** If improperly configured, these services can permit unauthorized access to user accounts and commands. (*d*)
- The firewall should restrict the following traffic types (TCP and UDP ports) to only specific systems where the service is necessary. (vii)

Telecommunications Security Controls (F) (continued)

Guidelines for Internet Security (3) (continued)

- **Simple mail transfer protocol (SMTP, port 25).** This service should only be allowed to specific mail servers. (*a*)
- **Routing information protocol (RIP, port 520).** This service should only be allowed between necessary systems. This service can be spoofed to redirect packet routing. (*b*)
- **Domain names system (DNS, port 53).** This system contains names of hosts and information about hosts that could be helpful to attackers and could be spoofed. (*c*)
- **UNIX-to-UNIX copy program (UUCP, port 540).** If improperly configured, this service can be used for unauthorized access. (*d*)

- The firewall should restrict the following traffic types (TCP and UDP ports) only to outgoing connection requests. This control measure works in concert with the measure to locate all public access systems logically outside the protected NRC networks. (viii)
  - **Telnet, port 23.** Incoming telnet access from the Internet to systems within the NRC networks should be restricted completely. Allow only outgoing connections. (*a*)
  - **File transfer protocol (FTP, ports 20 and 21).** Again, restrict FTP connections to outgoing requests. (*b*)
  - **Network news transfer protocol (NNTP, port 119).** This service is used for accessing and reading network news. (*c*)
  - **Information servers and World Wide Web (WWW) browser clients (gopher, port 70, and hypertext transfer protocol (http) port 80).** These should be restricted to outgoing connections only. (*d*)
- Physically and/or logically disconnect Internet workstations from NRC networks during periods of connection to the Internet, in cases where users of NRC networks also utilize dial-up serial line Internet protocol (SLIP) or point-to-point protocol (PPP) type connections to an external Internet access provider. (ix)
- Ensure virus checking is accomplished on any files received via download or email. (x)

Telecommunications Security Controls (F) (continued)

Guidelines for Internet Security (3) (continued)

- For NRC public access servers, ensure the following security measures are in place. (xi)
  - Ensure that all public access servers are connected solely to a public access portion of the network, logically outside of the NRC firewall capability so that the public cannot gain unauthorized access into NRC or other sensitive systems. (a)
  - Prohibit the use of "live" data, where feasible; use only copies of data for public access systems. (b)
  - Prohibit public users from reaching the operating system prompt. (c)
- Users should ensure that their browser software has been disabled to restrict the use of software, such as Active X and Java, that can dynamically download processes that have been initiated remotely to the client. (xii)

Information Security Controls (G)

Information security concerns all policies and safeguards provided to media used to process and store sensitive data. The following describes necessary actions in relation to AIS storage media (e.g., disks, backup tapes).

Documentation (1)

All documentation providing the technical parameters (e.g., system administrator manuals) of the AIS hardware- and software-based security features should be accounted for and controlled. Sensitive hardcopy documents, working papers, microfiche, and photographs should be stored in waterproof, fire-resistant locked filing cabinets or safes. Access is to be restricted to authorized personnel only.

Backup of AIS (2)

The following procedures should be implemented when backing up media. Compliance with these procedures will ensure that reliable backups are on hand in case there is a need for system or file recovery.

- **Purpose of Backups**. Backups should always be performed to allow for recovery of information that has been accidentally or maliciously destroyed. (a)

Information Security Controls (G) (continued)

Backup of AIS (2) (continued)

- **Backup Schedule.** A backup schedule should be created outlining the type of backup, the interval for each backup, the storage location and the number of copies of each backup. (b)
- **Full Backups.** Full backups should be performed on a weekly basis. A full backup typically includes the operating system, all applications, all the data from databases, and users' home directories. (c)
- **Incremental Backups.** Incremental backups should be performed on a nightly basis. Incremental backups are performed on directories or files that have been altered from the previous day. This can be detected by looking at the last date a file or directory has been accessed. Users' home directories and databases should be backed up nightly. (d)
- **Location of Full Backups.** At least two sets of full backups should be maintained. One backup should remain on site for conveniently recovering from minor problems. A second copy should be removed to an offsite storage facility immediately following its creation. This allows recovery from situations where the primary facility has been damaged or cannot be accessed. (e)
- **Backup Media.** Only high quality media (disk, tape, or optical read and write storage) should be used for backing up mission critical files. This will ensure good quality backups are available for recovery, should the need arise. (f)
- **Purging Files.** Before backing up, regularly purge unneeded files from the disk drives. The less data stored, the less storage space needed for backups, and the less time the backups will take. (g)
- **Timing of Backups.** Backups should be performed during periods of limited use, preferably at night. Wherever possible, scripts or batch programs should be created to automatically perform the backups on a certain date and time. Backup hardware devices normally include software that automates the backup process. (h)
- **Verification and Error Correction.** The maximum verification and error correction option should be selected whenever backups are performed. Although the backup takes a longer period of time, this ensures that all information is properly recorded, and that the information on the backup media is identical to the source data. (i)

Information Security Controls (G) (continued)

Backup of AIS (2) (continued)

- **User Backup Files.** Users of workstations on a LAN should usually store data on the LAN server as well as the hard disk of their workstation. For efficiency of operations, users should store all critical information on the server, allowing the data to be backed up each time the LAN Administrator backs up the server. To facilitate this process, home directories for each user should be created on the LAN server for their use in storing their critical data. (j)

- **Storage of Backups.** Both the onsite and offsite backups should be stored in a media library (if available) or in a waterproof and fireproof storage cabinet or safe. (k)

- **Testing of Storage Media.** Regular testing of storage media containing backed up sensitive data should be performed to ensure that they can be used effectively to restore sensitive information. (l)

Labeling of AIS Media (3)

The following procedures should be implemented to label media containing sensitive data. Labeling should identify the sensitivity level of the information contained within the media to facilitate proper storage of media. Compliance with these procedures reduces the risk of sensitive information being left in unauthorized places and reduces the chance of intentional disclosure, copying or destruction of the information.

- **Sensitive Media Marking.** All media containing sensitive information should be clearly labeled to indicate the sensitivity level of the most sensitive information contained on the media. The sensitivity level of the data should be clearly visible in human readable form on its exterior, electronically within the file containing the sensitive information, and on workstation, console, and PC monitor screens whenever sensitive information is displayed. (a)

- **Privacy Act Media.** Magnetic media containing Privacy Act data should be labeled with the following additional information: (b)

  - Privacy Act statement (wording to the effect that the information contained in the media is protected by the Privacy Act of 1974 and should be safeguarded against unauthorized disclosure) (i)

Information Security Controls (G) (continued)

Labeling of AIS Media (3) (continued)

- Retention period (ii)
- Destruction or deletion guidelines (iii)

- **Diskette Labeling.** Externally label all diskettes containing sensitive information to indicate sponsor, creation date, sensitivity level of the data contained, and a brief description of the data on the storage media. This information should be written in permanent ink on a gummed label affixed to the diskette itself. (c)
- **Placement of Labels.** The label should be placed on the media (diskette, microfiche sheet) itself, and if a protective sleeve is used, the label should be either visible through it, or the protective sleeve should be labeled. (d)
- **Copied Information.** If sensitive information is copied to storage media from a hard disk of a computer or from another network system, the media should assume the sensitivity level of the data that is copied onto it. When information is copied from one medium to another such as from a diskette to a computer or between computers directly and the media have different levels of security, both media shall assume the higher level of security and shall be labeled accordingly. (e)
- **Specification of Media Contents.** Special use diskettes, tapes, or optical storage media, such as media containing copies of data to be transported to another workstation, should be labeled to indicate what type of file(s) the media contains, any special instructions, and a point of contact. (f)
- **System Generated Labeling.** In the case of computer-generated documents, sensitivity labels should be system generated. (g)
- **Marking of Removable Media and Devices.** Removable AIS storage media and devices used with AIS should be marked on the front only, with appropriate markings to indicate the highest level of sensitive information contained therein. Pressure tape or labels may be used for this purpose. (h)
- **Marking of SGI and Classified Material.** For SGI, all media (e.g., diskettes, tapes, printouts) should be properly marked and stored in DFS-approved storage containers when not in use. For classified

Information Security Controls (G) (continued)

Labeling of AIS Media (3) (continued)

material, all media (e.g., diskettes, tapes, printouts, ribbons) should be properly labeled, stored, sanitized, and disposed of as specified in MD 12.2, "NRC Classified Information Security Program." (i)

Storage of AIS Media (4)

The following is a list of recommended procedures for properly controlling and handling storage media:

- **User Storage of Media.** Magnetic media produced and utilized by individual users on their workstations should be stored in locked desks or offices and should be afforded protection consistent with the security provided to sensitive information in hardcopy form. (a)

- **Operating System Media.** Media containing operating system information should not be issued to individuals other than system or network administrators. (b)

- **Prohibition Against Unattended Media.** Media containing sensitive information should not be left unattended in automobiles, at home, or in the workplace when not in use. (c)

- **Protection of Media From Heat and Cold.** All storage media should be stored away from extreme heat or cold, direct sunlight, extreme humidity, and strong magnetic fields, such as those generated by motors found in fans or office heating and cooling equipment. (d)

- **Use of Removable Hard Drives.** Whenever PCs are being considered for a stand-alone application, consideration should be given to the use of removable hard disk drives for storing sensitive information. This allows the hard disk to be removed and stored in a secure container. (e)

- **Protection Against Static Electricity.** Avoid using any plastic diskette containers that can generate static that will damage data. (f)

- **Write Protecting Diskettes.** All diskettes should be write-protected before their storage. This will ensure that sensitive data on the diskette is not accidentally overwritten. (g)

Information Security Controls (G) (continued)

Storage of AIS Media (4) (continued)

- **Protection of 5.25-Inch Diskettes**. To avoid damage to 5.25-inch diskettes, do not use rubber bands, staples, paper clips, or any other type fastener. When not in actual use, 5.25-inch diskettes should be stored in their protective sleeves. (h)

Destruction of Storage Media (5)

The following procedures should be implemented when any media containing sensitive information is to be disposed of or reused. Compliance with these guidelines reduces the risk of exposing sensitive information to the threat of disclosure or copying by unauthorized personnel.

- **Prohibitions on Destruction of Media**. Removable magnetic storage media, such as diskettes and tapes that contain classified or sensitive information, should not be disposed of in regular waste containers. This media should be sent to DFS for retention or destruction. (a)

- **Degaussing**. All magnetic storage media, such as hard disks, diskettes and magnetic tape, should be degaussed to remove sensitive information before discarding or reusing, thus preventing potentially sensitive or Privacy Act data from being disclosed to unauthorized persons. A manufacturer-recommended degausser product for the hardware or storage media should be used when degaussing. Contracting with an appropriate vendor for degaussing service may be an acceptable alternative to the purchase of degaussing equipment. (b)

- **Burning and Shredding of Media**. Should degaussing not be possible, media should be destroyed by burning or with a crosscut shredder approved for destruction of classified media. (c)

- **Overwriting Media**. Defective or damaged magnetic storage media that contains sensitive data should not be returned to the vendor who performs maintenance or repair, unless the vendor is contractually required to protect sensitive data. The sensitive data should first be overwritten before the media may be released to uncleared personnel. This also applies to media to which an unsuccessful attempt has been made to copy sensitive information. (d)

Information Security Controls (G) (continued)

Destruction of Storage Media (5) (continued)

- **Destruction of Defective Media.** Defective hard disk drives, diskettes, or magnetic tapes that contain sensitive information and that can not be erased by degaussing, should be destroyed by burning. (e)

- **Hard Disk Media.** If hard disk drives are removed from or replaced in a workstation, the hard drive that is removed should be unconditionally formatted before removal. If this is not possible, hard disks should be degaussed or sent to DFS for retention or destruction. (f)

- **Media Maintenance.** If computer systems containing sensitive unclassified information are to be sent out for service the hard drive should be removed before leaving the facility. The hard drive should be stored according to the level of sensitivity of the data processed on that system until the computer system is returned. (g)

- **Clearing System Memory.** Always clear sensitive information from the system memory of disk operating system (DOS) by turning off the computer for at least 1 minute. However, do not switch off UNIX, Novell NetWare, Windows NT, or OS/2 workstations without first performing the proper system shutdown sequence. (h)

Security Controls for AIS Processing SGI or Classified Data (H)

Security Controls for AIS Processing Unclassified SGI (1)

A system security plan (SSP) for an AIS processing unclassified SGI must be developed in accordance with the requirements of Part I(E) of this handbook. In addition to preparing the SSP, the SSO shall ensure that the following rules are enforced while processing unclassified SGI (see MD 12.6):

- The AIS must not use a hard disk for any data storage (intermediate results, final results, overflow, or backup) unless the AIS can be provided with adequate security for the open storage of such information and provision is made in the plan for sanitization or destruction of the hard drive if the AIS is to be removed from the protected area. (a)

Security Controls for AIS Processing SGI or Classified Data (H) (continued)

Security Controls for AIS Processing Unclassified SGI (1) (continued)

- The AIS, with the exception of those systems located in an NRC sensitive compartmented information facility (SCIF) or another DFS-approved facility, must be physically disconnected from LANs, modems, and shared printers. (b)

- The AIS must be protected in a manner that prevents unauthorized personnel from having visual access to the information being processed. This protection may be accomplished by screens, hoods, or positioning the equipment (monitors or printers) so that it faces away from doorways, windows, or open areas. (c)

- The AIS must never be left unattended when processing SGI. (d)

- All media (e.g., diskettes, tapes, printouts) must be properly marked and stored in DFS approved storage containers when not in use. (e)

- Disks, diskettes, ribbons and printouts must be disposed of in accordance with MD 12.6. (f)

- All users processing unclassified SGI shall follow current policy statements (e.g., NUREG/BR-0168, and Exhibit 3 of this handbook) from CSS regarding processing techniques using standard software protection features. (g)

Security Controls for AIS Processing Classified Information (2)

An SSP for an AIS processing classified information must be developed in accordance with the requirements of System Security Plan, Part I, Paragraph (E). In addition to preparing an SSP, the SSO shall ensure that the following rules are enforced while processing classified information (see MD 12.2).

- The AIS must not contain or use a permanent fixed disk for any data storage (intermediate results, final results, overflow, or backup) unless the AIS can be provided with adequate security for the open storage of such information and provision is made in the plan for sanitization or destruction of the hard drive if the AIS is to be removed from the protected area. (a)

Security Controls for AIS Processing SGI or Classified Data (H) (continued)

Security Controls for AIS Processing Classified Information (2) (continued)

- The AIS, with the exception of those systems located in an NRC SCIF or another DFS-approved facility, must be physically disconnected from LANs, modems, and shared printers. (b)
- The AIS must be protected in a manner that prevents unauthorized personnel from having visual access to the information being processed. This protection may be accomplished by screens, hoods, or positioning the equipment (monitors or printers) so that it faces away from doorways, windows, or open areas. (c)
- The AIS must never be left unattended when processing classified data. (d)
- All media (e.g., diskettes, tapes, printouts, ribbons) must be properly labeled, stored, sanitized, and disposed of as specified in MD 12.2. (e)
- All users of an AIS that has multiple users and which is used intermittently for classified processing must be recorded on a manual audit log. Logging for systems that are on line each day, located in protected facilities, and that are in existence expressly for classified processing, is not required. These logs must provide the following information: (f)
  - Date and time of day classified processing began (i)
  - Name of the user of the classified AIS (ii)
  - Date and time of day classified processing was completed (After classified processing has been completed, clear the AIS memory (sanitize it) by turning it off for at least 1 minute. Complete and sign the manual log entry. Store or destroy all classified media, as specified in MD 12.2.) (iii)
- An entry must be made indicating that the user verified that the previous user sanitized the AIS checking log entries. If the AIS was not sanitized, the user shall sanitize the AIS and will inform the previous user of the omission. If the previous user is not available, the user will notify the SSO. (iv)

Security Controls for AIS Processing SGI or Classified Data (H) (continued)

Security Controls for AIS Processing Classified Information (2) (continued)

- An entry must be made indicating the date and time of day the classified AIS was sanitized. (v)
- The user of the classified AIS must sign. (vi)

Abbreviations

ACL	Access control list
ADD	Applications Development Division (OCIO)
ADM	Office of Administration
ADP	Automatic data processing
AEA	Atomic Energy Act of 1945, as amended
AIS	Automated information system (used synonymously with IS)
AUTOS	Agency upgrade of technology for office systems
CIO	Chief Information Officer
COTS	Commercial off-the-shelf (software)
CPU	Central processing unit
CSS	Computer Security Staff (PRMD, OCIO)
DAC	Discretionary access control
DBMS	Database management system
DCPM	Division of Contracts and Property Management (ADM)
DES	Data Encryption Standard
DFS	Division of Facilities and Security (ADM)
DNS	Domain name system
DOE	Department of Energy
DOS	Disk operating system
FIPS	Federal Information Processing Standard
FTP	File transfer protocol
GSA	General Services Administration
HR	Office of Human Resources
HTTP	Hypertext transfer protocol
ID	(user) identification code
IP	Internet protocol
ISDN	Integrated services digital network
IT	Information technology
ITID	Information Technology Infrastructure Division (OCIO)
LAN	Local-area network

Abbreviations (continued)

MD	Management Directive
MDS	Management Directive System
NFS	Network file system
NIH	National Institutes of Health
NIS	Network information service
NIST	National Institute of Standards and Technology
NISTIR	National Institute of Standards and Technology Internal Report
NNTP	Network news transfer protocol
NSTISSC	National Security Telecommunications and Information Systems Security Committee
OCIO	Office of the Chief Information Officer
OMB	Office of Management and Budget
OSI	Open systems interconnection
PC	Personal computer
PERSEC	Personnel Security Branch (DFS, ADM)
PIN	Personal identification number
PPP	Point-to-point protocol
PRMD	Planning and Resource Management Division, OCIO
RIP	Routing information protocol
RPC	Remote procedure call
SCIF	Sensitive compartmented information facility
SDLCM	System Development Life Cycle Methodology
SGI	Unclassified safeguards information
SISS	Subcommittee for Information Systems Security
SLIP	Serial line internet protocol
SMTP	Simple mail transfer protocol
SSO	System security officer
SSP	System security plan
TCP	Transmission control protocol
TFTP	Trivial file transfer protocol
UDP	User datagram protocol
UUCP	UNIX-to-UNIX copy program
WAN	Wide-area network
WWW	World Wide Web

Glossary

Access. The ability and the means necessary to approach, to store or retrieve data, to communicate with, or to make use of any resource of an automatic data processing (ADP) system.

Access control. The process of limiting access to the resources of an ADP system only to authorized users, programs, processes, or other ADP systems (in computer networks).

Access control list (ACL). A discretionary access control mechanism that implements an access control matrix by representing the columns as lists of users attached to the protected objects.

Access privilege. The particular access permission (i.e., read, write, append, execute, delete, create, modify) granted to a subject in relation to an object.

Accountability. The quality or state that enables violations or attempted violations of ADP system security to be traced to individuals who may then be held responsible.

Accreditation. A formal declaration of the accrediting authority that an automated information system (AIS) is approved to operate in a particular security mode using a prescribed set of safeguards. Accreditation is the official management authorization for operation of an AIS and is based on the certification process as well as other management considerations. The accreditation statement affixes security responsibility with the accrediting authority and shows that due care has been taken for security.

Accreditation authority. The official who has the authority to decide on accepting the security safeguards prescribed for an AIS or that official who may be responsible for issuing an accreditation statement that records the decision to accept those safeguards.

Glossary (continued)

Application. The system, functional area, or problem to which a computer is applied. The application includes related manual procedures as well as automated procedures. Payroll, accounting, and management information systems are examples of applications.

Application software. A set of computer instructions designed to achieve a specified objective such as payroll, accounting, or management analysis. Application software may consist of operating system instructions or any programming language.

Application system. The organized collection, processing, transmission, and dissemination of information in accordance with defined procedures (automated or manual) to achieve a specific objective or function.

Assurance. A measure of confidence that the security features and architecture of an AIS accurately mediate and enforce the security policy.

Audit trail. A chronological record of system activities that is sufficient to enable the reconstruction, review, and examination of the sequence of environments and activities surrounding or leading to an operation, a procedure, or an event in the path of a transaction from its inception to output of final results.

Authentication. (1) The act of identifying or verifying the eligibility of a station, originator, or individual to access specific categories of information. (2) A measure designed to provide protection against fraudulent transmissions by establishing the validity of a transmission, message, station, or originator.

Authorization. The granting of access rights to users, processes, or programs.

Automated information system (AIS). An assembly of computer hardware, software and/or firmware configured to collect, create, communicate, compute, disseminate, process, store, and/or control data or information.

Glossary (continued)

Automated information system facility. One or more rooms (e.g., Two White Flint computer room, local-area network [LAN] equipment rooms), generally contiguous, containing the elements of an AIS system.

Automated information system (AIS) security. Measures and controls that protect an AIS against denial of service and unauthorized (accidental or intentional) disclosure, modification, or destruction of AIS and data. AIS security includes consideration of all hardware and/or software functions, characteristics, and/or features; operational procedures, accountability procedures, and access controls at the central computer facility, remote computer, and terminal facilities; management constraints; physical structures and devices; and personnel and communication controls needed to provide an acceptable level of risk for the AIS and for the data and information contained in the AIS. It includes the totality of security safeguards needed to provide an acceptable protection level for an AIS and for data handled by an AIS.

Availability. The state when AIS resources are in the place needed by the user at the time user needs them, and in the form needed by the user.

Backup. (1) A copy of a program or data file that is kept for reference in case the original is lost or destroyed. (2) Reserve computing capability available in case of equipment malfunction, destruction, or overload.

Certification. The comprehensive evaluation of the technical and nontechnical security features of an AIS and other safeguards, made in support of the accreditation process, that establishes the extent to which a particular design and implementation meet a specified set of security requirements.

Chief Information Officer (CIO). The NRC management official who is responsible for planning, directing, overseeing the delivery of centralized information technology infrastructure, applications, and in formation management services, and the development and implementation of plans, architecture, and policies to support the mission, goals, and priorities of the agency.

Glossary (continued)

Computer Security (i.e., network security, information systems security). The *cost-effective* protection of *sensitive* automated information from unauthorized disclosure, modification, misuse, loss, or denial of service.

Computer Security Staff (CSS). Office of Chief Information Officer (OCIO) computer security personnel located in the Planning and Resource Management Division (PRMD), who are responsible for the security of all AIS at NRC. Their primary responsibility is to enforce the NRC AIS security program. The CIO has been designated the accrediting authority for SGI, sensitive unclassified, and classified AIS for mainframes, minicomputers, and LANs. Microcomputer AIS should be certified by the system security officer (SSO) and accredited by the SSO's supervisor.

Confidentiality. The concept of holding sensitive data in confidence, limited to an appropriate set of individuals or organizations.

Configuration management. The management of security features and assurances through control of changes made to a system's hardware, software, firmware, documentation, test, test fixtures and test documentation throughout the development and operational life of the system.

Contingency plan. A plan for emergency response, backup operations, and post-disaster recovery maintained by an activity as part of its security program that will ensure the availability of critical resources and facilitate the continuity of operations in an emergency situation. Synonymous with *Disaster Recovery Plan*.

Cost-effective protection. The safeguards for a system are reasonably proportionate to the estimated risks (i.e., the potential harm or loss).

Countermeasure. Any action, device, procedure, technique, or other measure that reduces the vulnerability of or threat to a system. Synonymous with *Safeguard*.

Glossary (continued)

Criticality. The importance of an asset or system to an organization. The level of criticality is determined by the organization's need for asset/system availability, integrity, and confidentiality. The level of criticality is directly related to the level of security protection required.

Data. Programs, files, or other information stored in, or processed by, a computer system.

Data Encryption Standard (DES). A cryptographic algorithm for the protection of unclassified data, published in Federal Information Processing Standard (FIPS) 46. The DES, which was approved by the National Institute of Standards and Technology, is intended for public and Government use.

Data integrity. The property that data meet a prior expectation of quality. See also *System Integrity*.

Degausser. An electrical device that can generate a magnetic field for the purpose of degaussing magnetic storage media.

Denial of service. Any action or series of actions that prevent any part of a system from functioning in accordance with its intended purpose. This includes any action that causes unauthorized destruction, modification, or delay of service.

Destruction. The physical alteration of ADP system media or ADP system components such that they can no longer be used for storage or retrieval of information.

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

Disaster Recovery Plan. Synonymous with *Contingency Plan*.

Discretionary access control (DAC). A means of restricting access to objects based on the identity and need-to-know of the user, process, and/or groups to which they belong. The controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject.

Glossary (continued)

Domain. The unique context (e.g., access control parameters) in which a program is operating; in effect, the set of objects that a subject has the ability to access.

Encryption. The process of transforming data to an unintelligible form in such a way that the original data either cannot be obtained (one-way encryption) or cannot be obtained without using the inverse decryption process.

Environment. The aggregate of external procedures, conditions, and objects that affect the development, operation, and maintenance of a system.

Executive State. One of several states in which a system may operate and the only one in which certain privileged instructions may be executed. Such instructions cannot be executed when the system is operating in other (e.g., user) states. Synonymous with *supervisor state*.

General support system. These consist of hardware and software that provide general ADP or network support for a variety of users and applications. These systems include host computers (mainframes, minis, workstations) and networks local-area network (LANs and wide-area networks [WANs]). Even if none of the individual applications are sensitive, the support system may be considered sensitive, if overall, the aggregate of applications and support provided are critical to the mission of the agency.

Hard copy. Information that is printed on paper, slides, microfilm, or photographs. Not involving storage on magnetic media.

Identification. The process that enables recognition of an entity (user or process) by a system, generally by the use of unique machine-readable user names.

Identification and Authentication (I&A). The combination of a process that enables recognition of an entity by a system, generally by the use of unique machine-readable user names (identification) and the verification of 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 (authentication).

Glossary (continued)

Information Security. The result of any system of policies and procedures for identifying, controlling, and protecting from unauthorized disclosure, information whose protection is authorized by Executive order, statute, or regulation.

Information Technology (IT). The hardware and software operated by a Federal agency or by a contractor of a Federal agency or other organization that processes information on behalf of the Federal Government to accomplish a Federal function, regardless of the technology involved, whether computers, telecommunications, or others. It includes automatic data processing equipment as that term is defined in Section 111(a)(2) of the Federal Property and Administrative Services Act of 1949. For the purposes of this directive, automatic data processing and telecommunications activities related to certain critical national security missions, as defined in 44 U.S.C. 3502(2) and 10 U.S.C. 2315, are excluded.

Integrity. Sound, unimpaired, or perfect condition. See *Data integrity and System integrity*.

Label. See *Sensitivity Label*.

Labeling. A piece of information that represents the security level of an object and that describes the sensitivity of the information in the object.

Least Privilege. The principle that requires that each subject (i.e., user or process) 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.

Local-area network (LAN). An interconnected group of office automation systems or system components that are physically located within a small geographic area, such as a building or campus.

Logon. The procedure used to establish the identity of the user and the levels of authorization and access permitted.

Glossary (continued)

Magnetic media. Any data storage medium and related technology including diskettes and tapes, in which different patterns of magnetization are used to represent the values of stored bits or bytes.

Major application. The term means a *computerized* information system or application that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. These applications require special management oversight.

Malicious code. Hardware, software, or firmware that is intentionally included in a system for an unauthorized purpose (e.g., Trojan horse).

Need-to-know. The necessity for access to, knowledge of, or possession of specific information required to carry out official duties.

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 trees, and programs, as well as bits, bytes, words, fields, processors, video displays, keyboards, clocks, printers, and network nodes.

Office information technology (IT) coordinator. The office IT coordinator is the individual appointed by the office director to coordinate all aspects of data processing for the respective office with the OCIO. The coordinator will usually help the SSOs to determine computer security requirements for their respective offices and provide other advice. The coordinator should approve users' requests for additional facility access (NRC Form 380); and system upgrades and software. The coordinator may also perform other duties regarding virus checking and computer security awareness.

Optical storage media. Media which uses a source of coherent light—usually a semiconductor laser—to read and write the data, usually to an optical disk.

Glossary (continued)

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

Permissions. A description of the type of authorized interactions a subnet can have with an object. Examples include: read, write, execute, add, modify, and delete.

Personnel security. The procedures established to ensure that all personnel who have access to sensitive information have the required authority as well as appropriate clearances.

Physical security. The application of physical barriers and control procedures as preventive measures or countermeasures against threats to resources and sensitive information.

Privileged instructions. A set of instructions (e.g., interrupt handling or special computer instructions) to control features (such as storage protection features) that are generally executable only when the automated system is operating in the executive state.

Privileges. A set of authorizations/permissions granted by an authorized officer to an AIS user to perform certain operations.

Process. A program in execution.

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

Reliability. The probability of a given system performing its mission adequately for a specified period of time under the expected operating conditions.

Remnants. The residual magnetism that remains on magnetic storage media after degaussing. Can also mean any data remaining on ADP storage media after removal of the power.

Remote access. Sending and receiving data to and from a computer or controlling a computer with workstations or personal computers (PCs) connected through communications (e.g., telephone line).

Glossary (continued)

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. Risk analysis is part of risk management. The two general categories of risk analysis are quantitative (estimating risks in terms of dollar losses) and *qualitative* (empirical estimates of risk, e.g., high, medium, low).

Risk assessment. Synonymous with *Risk analysis*.

Risk management. The total process of identifying, controlling and eliminating or minimizing uncertain events that may affect system resources. It includes risk analysis, cost benefit analysis, selection, implementation, and test, security evaluation of safeguards, and overall security review.

Safeguards. 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.

Security measure. Elements of software, firmware, hardware, or procedures that are included in a system for the satisfaction of security specifications.

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

Security specifications. A detailed description of the safeguards required to protect a system.

Glossary (continued)

Sensitive application. An application that requires a degree of protection because it processes sensitive data (i.e., administrative, personnel, financial, or national security data) or because of the risk and magnitude of loss or harm that could result from improper operation or deliberate manipulation.

Sensitive compartmented information facility (SCIF). An accredited area, room, group of rooms, or installation where sensitive compartmented information (SCI) may be stored, used, discussed, and/or processed.

Sensitive information. A generic term used to identify information designated as classified, sensitive unclassified, or unclassified safeguard information (SGI).

Sensitivity label. The physical representation of the sensitivity level of information.

Sensitivity level. A designation, associated with information, indicating (1) the amount of harm that can be caused by the exposure of that information to an unauthorized user, (2) any formal access approvals that should be granted before granting access to that information, and (3) any specific handling restrictions placed on that information.

Sensitive system. A system or network that stores or processes sensitive information.

Sensitive unclassified information. Any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, U.S.C. (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

Glossary (continued)

Separation of duties. Assigning to separate individuals key duties such as authorizing, approving, and recording transactions, issuing or receiving assets, making payments, and reviewing or auditing to minimize the risk of loss. Internal control depends largely on the elimination of opportunities to conceal errors or irregularities. This in turn depends on the assignment of work so that no one individual controls all phases of an activity or transaction, thereby creating a situation that permits errors or irregularities to go undetected.

Software security. General purpose (executive, utility, or software development tools) and applications programs or routines that protect data handled by a system.

Subject. An active entity, generally in the form of a person, process, or device, that causes information to flow among objects or changes the system state. Technically, a process/domain pair.

Supervisor state. Synonymous with *Executive State.*

System administrator. That person responsible for the installation, operation, maintenance, and performance of a LAN or a WAN.

System integrity. The quality that a system has when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system. See also *Data integrity.*

Systems development and life cycle methodology (SDLCM). The SDLCM Methodology, as detailed in NRC Management Directive 2.5, "Application Systems Life Cycle Management," is a structured approach to designing, developing, deploying, maintaining, and decommissioning information systems. It addresses all aspects of an information systems solution from cradle to grave. It allows, and even encourages, flexibility within a clearly defined structure.

System security officer (SSO). An SSO is the individual who is primarily responsible for the security of an NRC AIS and the development of the AIS system security plan (SSP). The SSO also may be a user of the AIS. One SSO may be responsible for many AIS.

Glossary (continued)

System security plan (SSP). The Office of Management and Budget (OMB)-formatted document that identifies the system components, the sensitivity and risks, and the detailed, cost-effective safeguards to protect the system.

Telecommunications security. The protection that ensures the authenticity of telecommunications and that results from the application of measures taken to deny unauthorized persons information of value which might be derived from the acquisition of telecommunications. Telecommunications security includes crypto security, transmission security, emission security, and physical security of communications security material and information.

Threat. Any circumstance or event with the potential to cause harm to a system in the form of destruction, disclosure, modification of data, and/or denial of service.

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; for example, making a "blind copy" of a sensitive file for the creator of the Trojan-horse program. See also *Malicious code.*

Unclassified safeguards information (SGI). 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.

User. A person or process accessing an AIS either by direct connections (i.e., via workstations) or indirect connections (i.e., prepare input data or receive output).

User identification (ID). A unique symbol or character string that is used by a system to identify a specific user.

Glossary (continued)

Virus. A self-propagating Trojan horse, composed of mission component, a trigger component, and a self-propagating component. See also *Malicious code*.

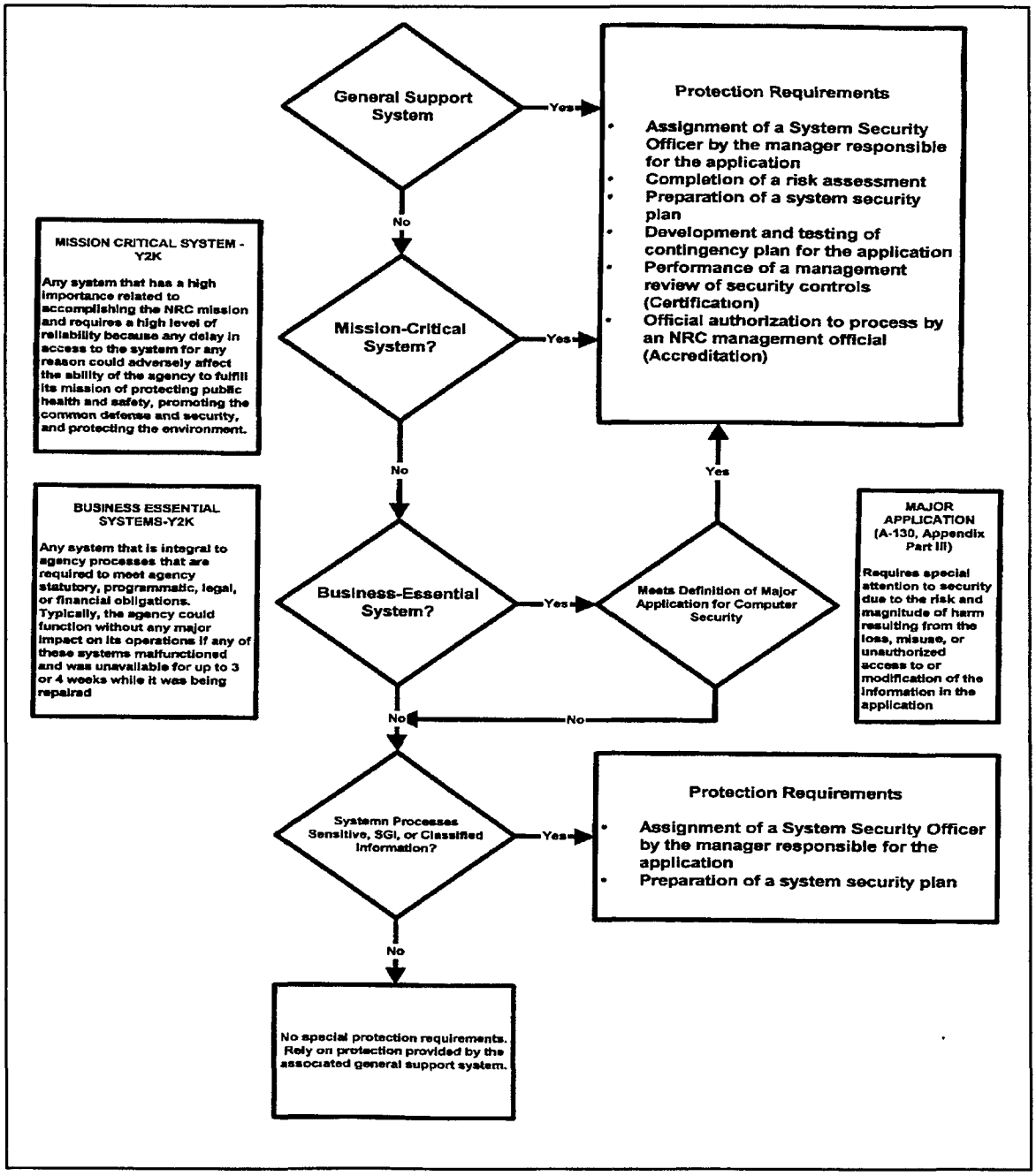
Vulnerability. A weakness in system security procedures, system design, implementation, internal controls, that could be exploited to violate system security policy.

Wide-area network (WAN). A collection of computing and communications devices, including local area networks, connected via a variety of transmission media, including telephone lines and other public networks, across a broad geographic area.

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

Exhibit 1

Determining Protection Requirements for Automated Information Systems (AIS)



Approved: May 2, 1995
(Revised: February 1, 1999)

Exhibit 2
Application Recovery Capabilities

The following application recovery capability levels have been developed as a guide for the implementation of contingency planning capabilities for NRC applications . They are out of necessity generic in nature and should only be used as a guide. A particular application in a specific operating environment may require more or less stringent capabilities depending on its criticality. The level of criticality of a given application should be determined in relation to other NRC applications through the use of a structured business impact analysis (BIA) methodology that is conducted on a periodic basis. These levels pertain to all NRC applications defined in Part I(A)(3) of the handbook.

It must be stressed that this is not a one size (or four sizes) fits all approach. Rather, the determination as to which level of a component is appropriate, depends on the criticality of the application, and the criticality of the application should be based on the results of a business impact analysis.

The levels should not be seen as a unified set of standards (i.e., for a given application). Level two may be appropriate for location of backups, but level three may be necessary for alternate processing availability. It is suggested that level three implementation be considered for "mission-critical" applications, as defined in the NRC Year 2000 program; that level two or three implementation be considered for NRC major applications and "business-essential" applications, as defined in the NRC Year 2000 program; and that level zero and one implementation be considered for other applications as defined in Part I(A)(3) of the handbook or "non-critical" applications, as defined in the NRC Year 2000 program.

Level Zero Capability: This level limits recovery capabilities to the default recovery capabilities that are provided by general support systems (e.g., data processing centers, local area networks, wide area networks, servers). Security at this level is provided at the discretion of the manager responsible for the general support system. Sponsors of applications that reside on Level Zero systems rely fully on the recovery capability offered by the general support system and do not implement additional, supplemental controls on their own and can anticipate a recovery capability at this level without taking additional actions on their own.

Level One Capability: In this level, full backups are taken weekly, and are stored in a locked container in the same building as the primary processor, but are separated from the primary processor. Two generations of the backups are maintained and stored in another building in the immediate vicinity, and a complete manual inventory of backup tapes is maintained. Documentation essential to the recovery of the application is inventoried and is backed up elsewhere in the facility. The alternate processing capability consists of an alternate system located in the same facility as the primary processor, which can process most of the critical applications or functions in a sequential fashion. The alternate processor can be available in 1 week. The contingency plan for the application has been developed but is incomplete because it provides only an outline of the application recovery organization, tasks, and

Exhibit 2 (continued)

resources. The plan is updated after testing is conducted. Recovery team members have been provided with overview training on the plan, and plan testing consists of quarterly checklist testing followed by simulation testing.

Level Two Capability: At this level, incremental backups taken daily, and full backups taken weekly. At least two generations of full backups are maintained, and seven generations of incremental backups are kept. Backups are stored in either a fire-rated vault in same facility or another building in the immediate vicinity. Read verifications of backups are conducted monthly, and essential documentation is inventoried and is available at a facility located elsewhere. An alternate system which can process all of the application's requirements is available within 72 hours in another building in the immediate vicinity. The application's contingency plan is generally up to date containing most but not all of the necessary information regarding recovery organization, tasks, and resources, and is updated on a quarterly basis. Personnel involved in the recovery of the application have been familiarized with their specific recovery roles, and contingency plan testing consists of annual parallel testing of a portion of the application following checklist and simulation testing.

Level Three Capability: This level of capability includes mirroring or parallel storage of backup data at a site at least 30 miles distant. Essential documentation is inventoried and is also available at another facility. An alternate system is available within 24 hours at a facility that is located at least 30 miles distant. This alternate system can support 100 percent of critical applications processing and a portion of the requirements for processing noncritical applications or functions. The application's contingency plan contains all necessary information regarding recovery organization, tasks, and resources, and recovery team members have been familiarized with their specific recovery roles. The application contingency plan is updated whenever a significant change to the application or related support staff occurs. Testing of the plan consists of annual parallel testing of the entire application capability preceded by checklist and simulation testing.

Note: At all Levels, basic system documentation, as defined in SDLCM, must be maintained.

Exhibit 2 (continued)

Application Recovery Capabilities Table

The following application recovery capability levels have been developed as a guide for the implementation of contingency planning capabilities for NRC applications. They are out of necessity generic in nature, and should only be used as a guide, since a particular application in a specific operating environment may require more or less stringent capabilities depending on its criticality. The level of criticality of a given application should be determined in relation to other NRC applications through the use of a structured business impact analysis (BIA) methodology that is conducted on a periodic basis. These four levels pertain to applications (e.g., major, other) defined in Section (A)(3) of this handbook.

Implementation Component	Implementation Level			
	Level 0	Level 1	Level 2	Level 3
Backups: Type	Accept capability provided by the general support system manager	Full	Full and incremental	Mirroring or parallel storage capability
Backups: Frequency	Accept capability provided by the general support system manager	Full backups taken weekly	Full backups taken weekly and incremental backups taken daily	Mirrored backups or electronic vaulting
Backups: Location	Accept capability provided by the general support system manager	Full backups stored in another building in the immediate vicinity	Full backups stored in another building in the immediate vicinity; incremental backups stored in the same building but separated from primary processor	Available in a facility at least 30 miles distant
Backups: Generations Maintained	Accept capability provided by the general support system manager	Two generations	Two generations of full backups, seven generations of incremental backups	Based on business requirements/records management policy
Backups: Testing	Accept capability provided by the general support system manager	Maintain complete inventory of tapes	Conduct read verification of backups monthly	Restore system quarterly using backups
Backups: Security	Accept capability provided by the general support system manager	Locked cabinet in same facility as primary processor	Fire–rated vault in another facility	Fire-rated vault in another facility
Contingency Plan: Maintenance	Accept capability provided by the general support system manager	Plan is updated following testing	Plan is updated following testing	Plan is updated continuously, to include updating following testing
Backups: Documentation	Accept capability provided by the general support system manager	Essential documentation is inventoried, and a backup set is available elsewhere in the facility	Essential documentation is inventoried, and a backup set is available another facility	Essential documentation is inventoried, and a backup set is available in another facility
Alternate Processing: Location	Accept capability provided by the general support system manager	Alternate system is in the same facility	Alternate system in another building in the immediate vicinity	Alternate system in a facility at least 30 miles distant

Exhibit 2 (continued)

Alternate Processing: Capacity	Accept capability provided by the general support system manager	Can process most critical applications/functions sequentially	Can simultaneously process all critical applications/functions	Can process all critical applications/ functions and a number of non-critical applications/ functions
Alternate Processing: Availability	Accept capability provided by the general support system manager	Available in one–four weeks	Available in 72 hours	Available in 24 hours
Contingency Plan: Development	Accept capability provided by the general support system manager	Plan provides only an outline of the system recovery organization, tasks, and resources	Plan contains much but not all of the necessary information regarding recovery organization, tasks, and resources	Plan contains all necessary information regarding recovery organization, tasks, and resources
Contingency Plan Training	Accept capability provided by the general support system manager	Team members have been provided with overview training	Team members have been familiarized with their specific recovery rules	Team members have been familiarized with their specific recovery roles
Contingency Plan: Testing Type	Accept capability provided by the general support system manager	Checklist testing and Simulation testing	Simulation Testing alternating with Checklist Testing	Parallel Testing alternating with Checklist and Simulation Testing
Contingency Plan: Testing Frequency	Accept capability provided by the general support system manager	Quarterly Checklist Testing followed by Simulation Testing	Parallel Testing annually on a portion of the system(s) preceded by a Checklist/ Simulation Test	Parallel Testing annually on the entire system(s) preceded by a Checklist/ Simulation Test

Exhibit 3
NetWare Security

System administrators should implement the following security parameters for each NRC Novell NetWare 3.x or 4.x system for which they are responsible. System passwords should be documented and stored in an approved security container

1 NetWare 3.X Security

1.1 Login Controls

The NetWare 3.x Intruder/Detection Lockout feature can be enabled to limit the number of unsuccessful login attempts a user is allowed to make. Following a predefined number of failed attempts, NetWare 3.x assumes that the user is an intruder and locks out the user for a predefined period of time.

After logging in to the server using an account with supervisor privileges, invoke the SYSCON utility. Choose "Supervisor Options" and "Intruder Detection/Lockout" from the menus, and ensure that the following parameters are set:

Detect Intruders:	Yes		
Intruder Detection Threshold:			
Incorrect Log in Attempts:	4		
Bad Log in Count Retention Time:	0 Days	1 Hours	0 Minutes
Lock Account After Detection:	Yes		
Length of Account Lockout:	3 Days	0 Hours	0 Minutes

1.2 Password Security

NetWare 3.11 and 3.12 systems should be configured to meet the Department of Defense "C2" security classification. This requires that Default Account Balance/Restrictions be configured using the SYSCON utility as follows:

Account Has Expiration Date:	No
Date Account Expires:	
Limit Concurrent Connections:	Yes
Maximum Connections:	1
Create Home Directory for User:	Yes
Require Password:	Yes
Minimum Password Length:	8
Force Periodic Password Change:	Yes
Days Between Forced Changes:	40
Limit Grace Logins:	Yes
Grace Logins Allowed:	1
Require Unique Passwords:	Yes
Account Balance:	0
Allow Unlimited Credit:	Yes
Low Balance Limit:	
Limit Server Disk Space:	No
Maximum Server Disk Space:	

1.3 Security Auditing

NetWare 3.x supervisors should run the SECURITY.EXE utility to determine the level of their system's security configuration. This utility generates a list of potential vulnerabilities in the network's security, checks the system's internal database (bindery) for user and group objects, and notifies the supervisor of potential problems due to excessive security imposed on a user or group, or due to unrestricted access because of a lack of passwords. The utility should be used to check on the following problems:

- Objects without assigned passwords
- Objects with insecure passwords (passwords that are easily guessed)
- Objects that have the security equivalence of Supervisor
- Objects with privileges in the root directory of a volume
- Objects without log in scripts
- Objects with excessive rights in standard directories

1.4 Server Console Security

NetWare 3.x has a server console security feature that can ensure that only certain users can access the server. The following NetWare features should be used:

Exhibit 3 (continued)

- **SECURE CONSOLE Command.** This should be issued at the server console to prevent loadable modules from being loaded from any directory other than SYS.SYSTEM. The feature also prevents anyone but the console operator from changing the system time and date, and it removes DOS from the file server.

- **Lock File Server Console.** Select this feature from MONITOR.NLM to implement password security on the console.

- **Remote Access Restriction.** Protect RCONSOLE.NLM with a password to prevent a user from accessing the console remotely.

2 NetWare 4.X Security

2.1 Log in and Password Controls

Using the NetWare 4.x Administrator Tool, log in restrictions should be set for each user account (object) to limit concurrent connections to one, but accounts should not be set to expire unless it is for a temporary employee or contractor with a known termination date. The following items should be checked in the Password Restrictions screen:

- Allow User to Change Password
- Require a Password (set minimum length to six)
- Force Periodic Password Changes (set days between forced changes to 90)
- Require Unique Passwords
- Limit Grace Logins (set grace logins allowed to one)

Using the Intruder Lockout option in the NetWare Administrator Tool, set the maximum number of incorrect log in attempts before lockout to three.

2.2 Auditing

NetWare 4.x system administrators should use the AUDITCON utility to audit activities on the system. Activities should be audited by event, by file/directory, and by user. At a minimum, all server (server shutdown, startup) and user (logins and logouts, trustee assignment changes, connection termination, disabling user accounts) events should be monitored. Events should also be audited depending on the resources available file (open/read/write file, create file/directory, and delete file/directory) and QMS (creating or deleting print queues).

NetWare 4.x audit events are logged to the NET$AUDT.DAT file. The system administrator should configure audit options relating to the generation of this audit file as shown below:

Exhibit 3 (continued)

Audit file maximum size:	Default or as required
Audit file threshold size:	Default or as required
Automatic audit file archiving:	Yes
Days between audit archives:	7 (or less)
Hour of day to archive:	As required
Number of old audit files to keep:	4
Allow concurrent auditor logins:	No
Broadcast errors to all users:	No
Force duel-level audit passwords:	No
Archive audit file:	Yes
Dismount volume:	No
Disable event recording:	No

Exhibit 4
Windows NT Security

System administrators should implement the following security parameters for each MicroSoft Windows NT system for which they are responsible.

1 User Identification and Authentication

1.1 **Unique User ID**. Assign each user a user identification code (user ID) and disable the *Guest* account.

1.2 **Enable Account** Lockout. Upon three consecutive invalid log in attempts, terminate the log in session and disable the account until the administrator resets it.

1.3 **Administrator Account**. Rename the *Administrator* account to one that can not be easily guessed, and restrict its use to the server console only.

1.4 **Do Not Allow Null Sessions**. For single domain environments, prevent access to NT's hidden *Anonymous* account by activating the anonymous user restriction feature provided in Service Pack 3. For multi-domain networks, evaluate the impact of activating the feature.

1.5 **User Passwords Minimum of Six Characters**. Require the use of strong passwords by implementing the password filtering option provided for Windows NT 4.0 by both Service Packs 2 and 3. This option will ensure that user passwords are at least six characters long, do not contain the user name or any part of the user name, and contain a combination of uppercase letters, lowercase letters, numerals, and special characters.

1.6 **Require System Administrator to Change Password**. Establish a policy to have system administrators change their passwords at least every 30 days.

1.7 **Prohibit Reuse of Passwords**. Configure the system to prohibit the reuse of the last six passwords. Additionally, set the system to require a minimum of seven days before the password can be changed to prevent users from cycling back to their "favorite" passwords.

1.8 **Encryption**. Implement the use of the 128 bit encryption system keys to protect the Security Accounts Manager (SAM) from attack by SAM database cracking software. System Administrators should ensure that the 128-bit encryption version of Service Pack 3 is installed rather than the standard 40-bit version..

2 Access Controls

2.1 **Access Rights**. Restrict the creating/modifying/deleting of access controls to authorized administrators only and sponsors of specific objects.

Exhibit 4 (continued)

2.2 **Group Accounts**. Ensure that the default *Everyone* group has read-only permission on the system root directory.

2.3 **Administrator Rights**. Ensure that rights to perform the following operations are restricted to administrators only:

- Backup files and directories
- Bypass traverse checking
- Change the system time
- Create a page file
- Debug programs
- Force shutdown from a remote system
- Generate security audits
- Load/unload device drivers
- Logon locally
- Manage auditing and security log
- Modify firmware environment variables
- Profile single process
- Profile system performance
- Restore files and directories
- Shutdown the system
- Take ownership of files and other objects

3 Auditing Controls

3.1 **Security Log Option**. Set the Security Log option to archive old events to protect them from being overwritten.

3.2 **Logging Events**. Ensure that the following events are recorded in the Security Log:

- All administrator activities
- Failed logon attempts
- Failed file and object access attempts
- Failed use of user rights
- Changes to user and group accounts
- Changes to security policy
- Restart/Shutdown of system

Exhibit 5
UNIX Security

The following security parameters should be implemented for each NRC UNIX-based system.

1 User Identification and Authentication

1.1 Password Controls

- All accounts should have a password or asterisk (*) placed in the password field.
- All vendor supplied passwords should be changed immediately.
- The following entry should not be in any */etc/passwd* or equivalent password file: +::0:0:::
- The shadow password file feature, if available, should be used to prevent copying of encrypted passwords by an intruder.
- All password management features (e.g., minimum length, aging) of the system should be utilized. Public domain and commercial password management programs (e.g., Password Coach, *npasswd, passwd+*) should be used to promote enforcement of password policies.

1.2 User Accounts

All user accounts should be carefully checked to ensure that duplicate user ID codes (numeric user IDs) are not assigned. UNIX access control decisions are based on the user ID and NOT on the account name.

2 Access Controls

2.1 Privileged Authority

Security controls for prudent use and protection of privileged authority, including root, should include:

- Proper justification of all assigned privileges;
- Use of other levels of privileged authority, other than root, if available on the system (e.g, SCO UNIX, AIX/ESA);
- Ensure that user ID=0 (root) is not assigned to non-root accounts; and
- Users should NOT be allowed to log in to a system directly as root, but should instead be required to log in using their real account name and then issue a switch-user (*su*) command to temporarily become privileged users.

Exhibit 5 (continued)

2.2 Access Modes

Standard UNIX access permission bit modes used with the *chmod* (change access modes) command for directory and file resources include:

Permission Mode	Octal	Symbolic
No permission	0	–
Execute only	1	x
Write only	2	w
Write and execute	3	wx
Read	4	r
Read/execute	5	rx
Read/write	6	rw
Read/write/execute	7	rwx

Note: Write permission at the directory level allows deletion and renaming of files contained therein, regardless of the permissions assigned at the file level.

Access permissions are applied for owner/group/all other users (world) for each resource, such as in the following example:

710: (7) = Owner has read/write/execute privileges,
(1) = Group has execute privileges,
(0) = All other users are allowed no access.

2.2.1 Home Directories. User HOME directories should be protected at mode=710 or 711.

2.2.2 User Umask Values. User unmask values should be set at mode=027 or 077.

2.2.3 System Resources Access. Recommended access permissions for system resources are:

- System directories: mode=755
- Publicly executable binary files: mode=751 or 711
- Public shell scripts: mode=775 or 755
- Security administration files: mode=750 or 700
- Sensitive system files (e.g., UUCP, system log): mode=750 or 700

Exhibit 5 (continued)

2.2.4 Modem Control Program Access. The access mode for modem control programs such as *cu* and *tip* should be tested for reliability (e.g., drop-off/add-on), and should be protected from unauthorized modification (use mode=600).

2.2.5 Device File Access. All device files (disk, memory, tape, and network) should be placed in the directory */dev*, should be owned by root, and should be protected at mode 600.

2.2.6 Use of Modes with Access Control Lists. Avoid use of chmod commands with octal (numeric) values if Access Control Lists (ACL) are in use (e.g., AIX systems).

2.3 Setuid/Setgid Controls

Controls for proper use of setuid/setgid should include:

- Limiting the number of *setuid/setgid* programs
- Assigning setgid instead of *setuid* where possible
- Inventorying and monitoring changes to *setuid/setgid* files
- Using only executable binary files (no scripts)
- Protection set at mode=511
- Properly designed error handling routines
- Proper resetting of user ID and group ID
- Sufficient documentation and testing
- Recording all *setuid/setgid* use in the audit logs

2.4 Protection of World-Writeable Directories

Use the "sticky bit" to protect world-writeable directories (e.g., temporary, mail) from unauthorized file deletion and renaming.

2.5 Group Level Access Controls

Use group level controls, wherever possible.

3 Utilities and Other Software

3.1 Execution of Untrusted Programs

Untrusted programs should not be run by root.

3.2 *Script*

The *script* command (recording program) should be removed.

3.3 Programs With Security Flaws

Programs with known security flaws should not be used. For example, the use of *sendmail* versions prior to 5.65, file transfer protocol server programs (*ftpd*) prior to 1/89, and *fingerd* programs prior to 12/88 should be avoided.

Exhibit 5 (continued)

3.4 *At* and *Cron*

Direct access to *at* and *cron* commands should be restricted to a limited number of trusted users and processes.

4 Network Services

4.1 *Finger*

Unwanted network services like *finger* should be removed (commented out with #) from the network configuration file (*etc/inetd.conf*).

4.2 *Rhosts*

The *.rhosts* file should NOT be used in directories of general users, should NOT contain "+", "+ +"(period space period), or " −", and should only be used for essential network management operations, containing only the names of trusted hosts which are directly involved in those operations (e.g., backup).

4.3 *Netrc*

The *.netrc* file should NOT be used if possible, but if needed, be protected at mode=600 to prevent disclosure of unencrypted passwords for other systems.

4.4 *Etc/hosts.equiv*

The */etc/hosts.equiv* file should NOT be used if possible, and if it must be used, it should not contain "+", "+ + " (period space period), or "−", or contain any user names.

4.5 Sendmail

The sendmail program should **not**:

- Have a wizard's password in the configuration file;
- Support debug, wiz, or kill commands;
- Deliver mail directly to a file or to a program; nor
- Deliver a file or execute a command that is encapsulated in an address.

4.6 Decode alias

The decode alias should be removed from the alias file(s).

Exhibit 5 (continued)

4.7 *File Transfer Protocol (FTP)*

The use of *FTP* should be limited. The */etc/ftpusers* file (list of users not authorized to use *FTP*) must contain, at a minimum, the following account names: root, uucp, nuucp, bin, and any other account that is not assigned to a general user.

4.8 *Anonymous FTP*

Anonymous FTP should not be permitted on computers with sensitive and/or critical resources.

4.9 *Trivial FTP (TFTP)*

TFTP should be used only on systems that require diskless booting, should be permitted to access only a limited number of files in a specific directory, and should be removed (disabled) if not needed along with other unnecessary network service entries from the */etc/inetd.conf file*.

4.10 *UUCP*

Safeguards for the *Unix-to-Unix Copy Program (UUCP)* should include the use of separate passwords for each system calling another system. Additional controls include:

- Using *HoneyDanBer UUCP* version 2.0 and later (also known as BNU - Basic Networking Utilities);
- Using *FTP* instead of *UUCP*;
- Assigning access privileges that allow remote systems to only access a limited number of specified directories and files, consistent with the proper use of the application(s);
- Prohibiting directory exportation;
- Limiting access to all *UUCP* control files (owned by root with no access allowed to general users); and
- Using the Permissions file to properly control and limit interactions with remote machines related to file access, remotely requested command execution, and logins.

4.11 Network Traffic Monitoring

To prevent general users from monitoring network traffic or finding out how the network is configured, the list of protected network management utility programs should include at a minimum *arp, ifconfig, netstat, ping*, and packet monitoring software (e.g., *snoop, tcpdump*).

Exhibit 5 (continued)

5 Audit Controls

5.1 Logged Data

Ensure that the system is configured to capture security audit log records (e.g., *syslog*) for successful and failed log in attempts, and if the feature is available, to present this information to the user upon each successful log in. Security audit log data for logins should be reviewed on a regular basis to identify any unusual activity that may be indicative of attempts to hack at the system.

5.2 Auditing *su*

All use of *su* should be logged by the system.

5.3 Recording Access Attempts

Use available security audit logging features to record failed file access attempts and all access attempts for selected sensitive files.

5.4 Use of Expert Systems

Use security/audit expert systems (e.g., COPS, DECInspect, ISS, Securemax, ASET, Raxco Security Toolkit) on a regular basis to identify and correct serious security exposures.

5.5 Monitoring Baseline Checksums

Maintain and periodically check baseline checksums for security sensitive files (e.g, setuid programs) to identify any unauthorized changes.

Exhibit 6
AUTOS Remote Access Agreement

1. Remote access directly into an individual office PC or micro computer is prohibited.

2. Remote access into the AUTOS local-area network (LAN) is permitted, but access is restricted to only official NRC work. No unofficial use can or will be authorized.

3. Remote access to classified information is prohibited.

4. Remote access to safeguards information is prohibited.

5. Remote access to sensitive unclassified data is permitted according to the provisions contained in NUREG/BR-0168, "Security Policy for Processing and Handling of Sensitive Unclassified Information in the AUTOS/Local-Area Network Environment."

6. Assigned account names and passwords are solely for use by account owners. They must be protected from unauthorized use at all times. Unauthorized use includes use by anyone other than the account owner, including other NRC staff or NRC contractors.

7. The user is responsible for the security and integrity of the NRC information and files according to Federal regulations and NRC policy.

8. NRC-issued computers and software are Government property and must be handled appropriately.

9. The NRC assumes no liability for supplies, loss, or damage to non-NRC owned equipment. Any NRC property that is lost, damaged or suspected stolen should be reported to the Division of Security, Office of Administration.

10. All user diskettes must be scanned for viruses before and after use. Contractors should be especially concerned with this matter.

11. No login scripts or account passwords shall be stored on PCs.

12. Employees who misuse NRC property maybe subject to disciplinary action.

U.S. NUCLEAR REGULATORY COMMISSION

DIRECTIVE TRANSMITTAL

TN: DT-99-33

To:	NRC Management Directives Custodians
Subject:	Transmittal of Directive 12.6, "NRC Sensitive Unclassified Information Security Program"
Purpose:	Directive and Handbook 12.6 have been revised to cross-reference MD 3.4, "Release of Information to the Public," and to include the use of Official Use Only cover sheets to facilitate identification or protection of unclassified information within NRC.
Office and Division of Origin:	Office of Administration
Contact:	Rhonda C. Bethea, 301-415-2254
Date Approved:	June 2, 1998 (**Revised: December 20, 1999**)
Volume:	12 Security
Directive:	12.6 "NRC Sensitive Unclassified Information Security Program"
Availability:	Rules and Directives Branch Office of Administration David L. Meyer (301)415-7162 or Jeannette P. Kiminas (301)415-7086

NRC Sensitive Unclassified Information Security Program

Directive 12.6

Contents

Policy 1

Objective 1

Organizational Responsibilities and Delegations of Authority 1

- Executive Director for Operations (EDO) 1
- Chief Information Officer (CIO) 2
- Inspector General (IG) 2
- Deputy Executive Director for Management Services (DEDM) 2
- Director, Office of Administration (ADM) 2
- Office Directors and Regional Administrators 2
- Director, Division of Facilities and Security (DFS), ADM 3

Applicability 3

Handbook 3

Exceptions or Deviations 3

References 3

NRC Sensitive Unclassified Information Security Program Directive 12.6

Policy
(12.6-01)

All U.S. Nuclear Regulatory Commission personnel responsible for the safeguarding of sensitive unclassified information (e.g., Official Use Only information and unclassified Safeguards Information), other sensitive information, and activities involving this information must adhere to the authorities, responsibilities, and procedures specified in this directive and handbook. This directive and handbook do not affect Commission rules and regulations contained in the *Code of Federal Regulations* that are applicable to NRC licensees and others.

Objective
(12.6-02)

To ensure that sensitive unclassified information is handled appropriately and is protected from unauthorized disclosure under pertinent laws, management directives, and applicable directives of other Federal agencies and organizations.

Organizational Responsibilities and Delegations of Authority
(12.6-03)

Executive Director for Operations (EDO)
(031)

Acts on appeals for denial of information requested under the Freedom of Information Act (FOIA) when the request involves information generated by offices reporting to the EDO, and acts on all appeals for denial of information requested under the Privacy Act.

Chief Information Officer (CIO)
(032)

Directs and oversees NRC's information resources and information management.

Inspector General (IG)
(033)

Investigates instances of improper disclosure of information in violation of statutes and regulations.

Deputy Executive Director for Management Services (DEDM)
(034)

As designated Senior Agency Official for information security matters, directs and administers the agency's information security programs.

Director, Office of Administration (ADM)
(035)

Provides overall NRC security program guidance and direction and ensures that NRC's security program is effectively and efficiently carried out by the NRC Division of Facilities and Security (DFS).

Office Directors and Regional Administrators
(036)

- Ensure that NRC employees and NRC contractor personnel under their jurisdiction are cognizant of and comply with the provisions of this directive and handbook. (a)
- Advise DFS of any existing or proposed sensitive unclassified activities in organizations under their jurisdiction. Report any significant change or termination of sensitive unclassified activities to DFS for review of associated contracts, subcontracts, or similar actions. (b)
- Advise DFS of any information that indicates noncompliance with this directive and handbook or is otherwise pertinent to the proper protection of sensitive unclassified information. (c)
- Request exceptions to or deviations from this directive and handbook, as required. (d)

Director, Division of Facilities and Security (DFS), ADM
(037)

Plans, develops, establishes, and administers policies, standards, and procedures for the NRC Sensitive Unclassified Information Security Program. Monitors reports of non-compliance and recommends corrective actions, as appropriate, to DEDM and office directors.

Applicability
(12.6-04)

This directive and handbook apply to all NRC employees and consultants and to all NRC contractors to whom they apply as a condition of a contract or a purchase order.

Handbook
(12.6-05)

Handbook 12.6 provides guidelines for the preparation, distribution, accountability, and safeguarding of sensitive unclassified information.

Exceptions or Deviations
(12.6-06)

Exceptions to or deviations from this directive and handbook may be granted by DFS except in those areas in which the responsibility or authority is vested solely with the Commission, the EDO, or with ADM, and is nondelegable; or for matters specifically required by law, Executive order, or directive to be referred to other management officials.

References
(12.6-07)

Atomic Energy Act of 1954, as amended (42 U.S.C. 2011 et seq.).

Code of Federal Regulations—

10 CFR Part 2, "Rules of Practice for Domestic Licensing Proceedings and Issuance of Orders."

10 CFR Part 9, "Public Records."

10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities."

10 CFR Part 51, "Environmental Protection Regulations for Domestic Licensing and Related Regulatory Functions."

References
(12.6-07) (continued)

10 CFR Part 70, "Domestic Licensing of Special Nuclear Material."

10 CFR Part 71, "Packaging and Transportation of Radioactive Material."

10 CFR 73.21, "Requirements for the Protection of Safeguards Information."

10 CFR 73.57, "Requirements for Criminal History Checks of Individuals Granted Unescorted Access to a Nuclear Power Facility or Access to Safeguards Information by Power Reactor Licensees."

10 CFR 73.71, "Reporting of Safeguards Events."

10 CFR Part 1017, "Identification and Protection of Unclassified Controlled Nuclear Information" (Department of Energy, General Provisions).

Energy Reorganization Act of 1974, as amended (42 U.S.C. 5801 et seq.).

"Freedom of Information Act" (5 U.S.C. 552).

Inspector General Act (5 U.S.C. App. 3).

NRC Management Directive 3.1, "Freedom of Information Act."

3.2, "Privacy Act."

3.4, "Release of Information to the Public."

3.5, "Public Attendance at Certain Meetings Involving the NRC Staff."

5.5, "Public Affairs Program."

12.1, "NRC Facility Security Program."

12.2, "NRC Classified Information Security Program."

12.3, "NRC Personnel Security Program."

12.4, "NRC Telecommunications Systems Security Program."

12.5, "NRC Automated Information Systems Security Program."

NUREG-0910, Rev. 3, "NRC Comprehensive Records Disposition Schedule."

NUREG-0794, "Protection of Unclassified Safeguards Information" (October 1981).

References

(12.6-07) (continued)

NUREG/BR-0069, Rev. 2, "NRC Classification Guide for National Security Information Concerning Nuclear Materials and Facilities" (CG-NMF-2) (December 1991).

"Privacy Act" (5 U.S.C. 552a).

NRC Sensitive Unclassified Information Security Program

Handbook 12.6

Contents

Part I

Introduction 1

Purpose and Scope (A) 1
Applicability (B) 1
Authority for Controls (C) 2
Authority To Designate Sensitive Unclassified Information (D) 2
Release of Information to the Public (E) 2
Sensitive Unclassified Records in ADAMS (F) 3

Part II

Proctection and Control of Sensitive Unclassified Information 4

Information Originated by NRC, NRC Contractors, or NRC Licensees (A) 4
Access (1) 4
When Information Is Marked (2) 6
How Information Is Marked (3) 7
Cover Sheet (4) 10
Reproduction (5) 10
Transmission (6) 11
Telecommunications (7) 13
Automatic Data Processing (ADP) (8) 15
Word Processing (9) 15
Protection of Information During Use (10) 15
Storage (11) 15
Destruction (12) 17
Removal of Information From the Sensitive Unclassified Category (13) 17
Information Originated by Sources Other Than NRC, NRC Contractors, or NRC Licensees (B) 21
General Rule (1) 21
Access (2) 22
Hearings, Conferences, or Discussions (C) 22
Security Preparations Required for Hearings, Conferences, or Discussions (1) 22
Where Held (2) 22
Protective Orders (D) 23

Contents (continued)

Exhibits

1 Safeguards Information 24
2 Information Not Subject to Safeguards Information (SGI) Controls 26
3 Safeguards Information Document Marking 27
4 Safeguards Information Cover Sheet 28
5 Proprietary Information Cover Sheet 29
6 Official Use Only Information Cover Sheet 30

Part I
Introduction

Purpose and Scope (A)

Requirements and procedures are given to ensure that sensitive unclassified information is adequately protected from unauthorized disclosure. (1)

"Sensitive unclassified information" is unclassified Safeguards Information (SGI), Official Use Only information, and Proprietary information. It also includes unclassified information from other Government agencies and sources outside of NRC and its contractors and licensees that requires special protective measures. Markings used by these agencies and sources include, for example, *For Official Use Only, Company Confidential*, and *Private*. (See Management Directive (MD) 12.4, "NRC Telecommunications Systems Security Program," and Volume 12, "Glossary," for a complete definition of "Sensitive Unclassified Information.") (2)

The provisions of this part apply to information determined or verified by NRC to be Proprietary and information said to be Proprietary. The use of the words "sensitive unclassified information" or "Proprietary" includes both information determined or verified by NRC to be Proprietary and information said to be Proprietary. (3)

The specific types of information and documents that constitute SGI are specified in Exhibit 1 to this handbook. This list is not intended to be all-inclusive. Exhibit 2 specifies types of information not subject to SGI controls. (4)

Applicability (B)

NRC employees, consultants, and contractors are responsible for ensuring that the procedures specified in this part are followed to protect sensitive unclassified information. The use of the word "contractor" in this part includes subcontractors.

Authority for Controls (C)

The primary authorities for the protection of sensitive unclassified information are the Freedom of Information Act (5 U.S.C. 552), the Privacy Act (5 U.S.C. 552a), and 10 CFR Parts 2 and 9. SGI is controlled in accordance with Section 147 of the Atomic Energy Act of 1954, as amended, and 10 CFR 73.21.

Authority To Designate Sensitive Unclassified Information (D)

To designate information as "sensitive unclassified," a determination must be made that one or more of the statutes and/or regulations mentioned in Section (C) of this part apply. This designation signifies that the information must receive limited distribution and must be protected from unauthorized disclosure. For matters of the Office of the Inspector General, the Inspector General is the only official authorized to designate documents as sensitive unclassified information under applicable statutes. (1)

Within NRC, branch chiefs and above, or other level deemed appropriate by an office director and issued in writing, are authorized to designate information as SGI. Within contractor organizations, the NRC contracting office's authorized representative or the NRC project officer, when necessary, authorizes employees to perform this function. (2)

NRC branch chiefs and above and personnel appointed by NRC contractors are authorized to designate information as "Official Use Only" or "Proprietary." (3)

Release of Information to the Public (E)

The presence of markings such as "Safeguards Information," "Official Use Only," "Proprietary," or other similar markings, or the lack of markings does not determine whether a document may be withheld from the public. A review must be made of each sensitive unclassified document requested to determine whether the document is releasable. (See MD 3.4, "Release of Information to the Public.") (1)

Whenever an office has a question regarding releasability, it may be appropriate to consult with—(2)

Release of Information to the Public (E) (continued)

- The Division of Information Management, Office of the Chief Information Officer (OCIO), if the Freedom of Information Act (FOIA) or the Privacy Act is involved (see MDs 3.1, "Freedom of Information Act," and 3.2, "Privacy Act") or the release of information relates to the NRC's public health and safety mission (see MD 3.4, "Release of Information to the Public") (a)
- The Office of Nuclear Material Safety and Safeguards on whether a document contains SGI (b)
- The Office of Nuclear Reactor Regulation on safeguards technical and regulatory reviews or generic reactor safeguards issues (c)
- The Office of the General Counsel on legal questions (d)
- Other responsible offices within NRC (e)
- The originator (f)

Other Government agencies or other sources should be consulted before documents bearing restrictive markings or containing sensitive unclassified information of primary interest to them are released to the public. (3)

When sensitive unclassified documents are requested under FOIA or the Privacy Act, the Freedom of Information Act and Privacy Act Officer, OCIO, will assist offices in determining if the documents fall within the scope of the request and consult with other Federal agencies or other sources from which the information is derived regarding their documents or information in NRC files. (See MDs 3.2, "Privacy Act," and 3.1, "Freedom of Information Act.") (4)

Sensitive Unclassified Records in ADAMS (F)

Documents created in the Agencywide Documents Access and Management System (ADAMS) containing or said to contain Proprietary information must be generated using the Proprietary template. For Official Use Only information, use the Official Use Only template to facilitate identification or protection of the information. The template should be used to safeguard unclassified information that may be exempted from public disclosure under FOIA or the Privacy Act and may be used to protect other unclassified information subject to conditional release (e.g., predecisional information). SGI may not be placed in ADAMS.

Part II

Protection and Control of Sensitive Unclassified Information

Information Originated by NRC, NRC Contractors, or NRC Licensees (A)

The procedures set forth in this section apply to Safeguards Information (SGI), Official Use Only, and Proprietary information.

Access (1)

NRC personnel and NRC contractor employees shall furnish sensitive unclassified information to only those persons who need the information for the conduct of official business. (a)

If doubt exists as to whether it is proper to furnish information in any particular case, NRC personnel and NRC contractor employees shall consult the—(b)

- Originating office (If the information was originated by a contractor or a licensee, the originator or the NRC office administering the contract or license must be consulted.) (i)
- Office that has primary interest in the information (ii)
- Source from which the information was derived (iii)

If SGI is involved, NRC personnel or NRC contractor employees shall consult the Office of Nuclear Material Safety and Safeguards and the Office of Nuclear Reactor Regulation. (c)

If Proprietary or Official Use Only information is involved, NRC personnel or NRC contractor employees shall consult the—(d)

Information Originated by NRC, NRC Contractors, or NRC Licensees (A) (continued)

Access (1) (continued)

- NRC office originating the information (i)
- Office that has primary interest in the information (ii)
- Source from which the information was derived (iii)

An access authorization (security clearance) is not required for access to SGI or other sensitive unclassified information. However, the requirements of 10 CFR 73.57 mandate an FBI fingerprint check be conducted for access to SGI at a power reactor facility. (e)

No person may have access to SGI unless the person needs the information to conduct official business and the person is—(f)

- An employee, agent, or contractor of an applicant for a license, of an NRC licensee, of the NRC, or of the United States Government (i)
- A member of a duly authorized committee of the Congress (ii)
- The Governor of a State or his or her designated representative (iii)
- A representative of the International Atomic Energy Agency (IAEA) engaged in activities associated with the U.S./IAEA Safeguards Agreement who has been certified by the NRC (iv)
- A member of a State or local law enforcement authority that is responsible for responding to requests for assistance during safeguards emergencies (v)
- An individual to whom disclosure is ordered in accordance with 10 CFR 2.744(e) in connection with a domestic licensing proceeding (vi)

The office director or the regional administrator responsible for the document may authorize additional distribution of SGI related to activities conducted under the license. The individuals specified in the preceding list are normally considered to be trustworthy in view of their employment status. However, some discretion should be used in granting access if there is any indication that the proposed recipient would be unwilling or unable to provide the protection prescribed for SGI. (g)

Information Originated by NRC, NRC Contractors, or NRC Licensees (A) (continued)

When Information Is Marked (2)

Documents (including drafts and worksheets), other than for Official Use Only that contain sensitive unclassified information and require marking, must be marked upon origination.

SGI Documents (a)

Documents (including drafts and worksheets) known to contain SGI that are not so marked must be marked accordingly by persons authorized to designate information as "Safeguards Information."

- Documents dated before January 20, 1981, need not be marked until they are withdrawn from the files. (i)
- Documents dated before January 20, 1982, and clearly marked as 10 CFR 2.790(d) to indicate that they contain SGI must be secured as SGI without the alteration of their marking until they are withdrawn from the files for any reason. When withdrawn, these documents must be marked in accordance with this part. (ii)

Official Use Only Documents (b)

A document that contains information for Official Use Only must be marked when the originator believes that marking is essential to ensure proper handling and to ensure that all persons having access to the record will be aware that the—

- Document must not be publicly released. (i)
- Document must be distributed only to those who have a need-to-know to conduct official business. (ii)

Conditional Release Documents (c)

Some NRC documents may be released to the public when particular conditions have been met (e.g., a particular period of time has elapsed, a particular event has occurred, or an agency position has been officially approved). These documents are subject to conditional release and should be protected as Official Use Only until the specific condition has been met. While physical marking of conditional release documents may not be appropriate and is not required, the use of cover sheets marked "Official Use Only" is encouraged to facilitate their protection until they meet the condition for public release.

Information Originated by NRC, NRC Contractors, or NRC Licensees (A) (continued)

When Information Is Marked (2) (continued)

Proprietary Information Documents (d)

Documents received by NRC or NRC contractors that contain or are said to contain Proprietary information but that are not marked must be marked when marking is essential to ensure proper handling and to ensure that all persons having access to the information will be aware that the—

- Information must not be publicly released. (i)
- Information must be distributed only to those who have a need-to-know to conduct official business. (ii)

How Information Is Marked (3)

Safeguards Information (a)

At the time it is determined that a document contains SGI, originators must place the name, title, organization, signature, and date of the individual authorized to make an SGI determination and who has determined that the document contains SGI in the lower right corner of the face of the original document, as indicated in Exhibit 3 of this handbook. If the originator or approver of the document is the person authorized to make the determination and signs the document, that signature is sufficient. The signature in either case must appear on the face of the original copy of the document. Other copies may have a facsimile signature or a typed name. (i)

For a document containing SGI, originators must place the marking "SAFEGUARDS INFORMATION" conspicuously at the top and bottom of the page. Originators also must place the marking "Violation of protection requirements for SAFEGUARDS INFORMATION subject to CIVIL and CRIMINAL penalties" in the lower left corner of the face of the document. (ii)

Official Use Only (b)

Originators must place the marking "OFFICIAL USE ONLY" at the top and bottom of the page on the face of each document containing information for Official Use Only when that marking is required to

Information Originated by NRC, NRC Contractors, or NRC Licensees (A) (continued)

How Information Is Marked (3) (continued)

ensure proper handling. The marking "LIMITED INTERNAL DISTRIBUTION PERMITTED" must be placed in the lower left corner of the face of the document.

Proprietary Information (c)

Originators must place the words "PROPRIETARY INFORMATION" at the top and bottom of the page on the face of each document containing or said to contain Proprietary information.

Multiple Page Documents (d)

The "SAFEGUARDS INFORMATION, OFFICIAL USE ONLY," or "PROPRIETARY INFORMATION" markings must be placed at the top and bottom of—

- The outside of the front and back covers, if any (i)
- The title page, if any (ii)
- The first page of text, if there is no front cover or title page (iii)
- The outside of the back page, if there is no back cover (iv)
- Each page of a document containing sensitive unclassified information (v)

Portion-Marking (e)

Portion-marking is accomplished by clearly indicating the portions (e.g., titles, paragraphs, subjects, or pages) that contain sensitive unclassified information by placing the appropriate abbreviation (e.g., "SGI") in parentheses at the beginning or end of the portion.

Sensitive Unclassified Information (i)

Portion-marking is required for sensitive unclassified information when—

Information Originated by NRC, NRC Contractors, or NRC Licensees (A) (continued)

How Information Is Marked (3) (continued)

- A document contains several categories of sensitive unclassified information. Portion-marking indicates which portions (e.g., paragraphs, pages, and appendices) contain each category, that is, Safeguards Information, SGI; Official Use Only information, OUO; or Proprietary information, "PROPIN." The highest category of information contained in the document ("SGI" or in the absence of "SGI," "PROPIN") will be the overall marking used at the top and bottom of the portion. (*a*)
- A document contains both classified and sensitive unclassified information. Portion-marking indicates which portions contain each category. Portions (e.g., paragraphs) that contain both sensitive unclassified information and classified information must be marked with the applicable classification markings only (see Part I, Section (B)(3)(g) of Handbook 12.2, "NRC Classified Information Security Program"). If a document is declassified and sensitive unclassified information remains, the document must be marked in accordance with the requirements stated in this part. (*b*)

Safeguards Information (ii)

In addition to the overall marking, portion-marking is required for SGI contained in—

- Correspondence to and from the NRC, NRC contractors, and NRC licensees (*a*)
- Items listed in Exhibit 1 of this handbook (*b*)

Files or Folders (f)

Files and folders containing sensitive unclassified information must be marked front and back with the appropriate category marking (e.g., "SAFEGUARDS INFORMATION," "OFFICIAL USE ONLY INFORMATION," or "PROPRIETARY INFORMATION") upon creation or when extracted from an existing file system.

Transmittal Documents (g)

Documents (e.g., cover letters or memoranda) that do not in themselves contain sensitive unclassified information but are used to

Information Originated by NRC, NRC Contractors, or NRC Licensees (A) (continued)

How Information Is Marked (3) (continued)

transmit one or more documents containing this information must be marked to indicate the fact that sensitive unclassified information is contained in the documents transmitted. The marking (e.g., "SAFEGUARDS INFORMATION," "OFFICIAL USE ONLY," or "PROPRIETARY INFORMATION") indicating the category of information must be placed at the top and bottom of the first page of the transmittal document. Additionally, the following marking must be placed at the side or bottom of the transmittal document:

> "Document transmitted herewith contains sensitive unclassified information. When separated from enclosures, this document is decontrolled."

Cover Sheet (4)

Each copy of a document containing SGI in the possession of NRC or NRC contractors must be covered by an SGI cover sheet (NRC Form 461, Exhibit 4). Documents containing or said to contain Proprietary information must be covered by a Proprietary information cover sheet (NRC Form 190, Exhibit 5), when necessary to prevent unauthorized access. (a)

Cover sheets should be used for Official Use Only information when their use facilitates identification or protection of the information. The Official Use Only cover sheet (NRC Form 190(x), Exhibit 6) should be used to safeguard unclassified information and may be used to identify and protect other information subject to conditional release. Cover sheets need not be used on documents that are in files. (b)

Reproduction (5)

A minimum number of copies of documents containing or said to contain sensitive unclassified information may be reproduced by holders to meet operational requirements without permission of the originator or the responsible office. Care must be taken to prevent unauthorized access during reproduction and in the disposition of matter containing sensitive unclassified information (e.g., unneeded copies or improperly prepared copies). (a)

Information Originated by NRC, NRC Contractors, or NRC Licensees (A) (continued)

Reproduction (5) (continued)

Whenever the originator wants to limit the further dissemination or reproduction of documents containing sensitive information, the following statement should be placed on the front of the document: "Reproduction or Further Dissemination Requires Approval of _____." (b)

If reproduction of sensitive unclassified information is requested, NRC Form 30, "Request for Administrative Services," or NRC Form 460, "Request for Graphics Services," should contain an explanation in the special instructions block that sensitive unclassified information is attached, and an asterisk should be placed in the "Unclassified" and "Other" blocks. This action must be taken to ensure proper handling of the document and proper disposal of any waste (see Section (A)(12) of this part). The requester shall ensure that the markings on documents submitted for reproduction are in black or red and dark enough to be reproduced. (c)

Transmission (6)

Methods Used (a)

Documents containing sensitive unclassified information must be transmitted by one of the following methods: (i)

- NRC messenger or NRC contractor authorized messenger or courier. NRC messengers and couriers shall be authorized to hand-carry sensitive unclassified information outside a facility by their division director or a higher level authority. NRC contractor personnel shall be authorized by the cognizant security office. (*a*)
- U.S. Postal Service First Class Mail, U.S. Postal Service Registered Mail, U.S. Postal Service Express Mail, or U.S. Postal Service Certified Mail (*b*)
- NRC headquarters interoffice mail or NRC pouch mail between NRC headquarters and regional offices (*c*)

Information Originated by NRC, NRC Contractors, or NRC Licensees (A) (continued)

Transmission (6) (continued)

- Any individual authorized access to the category of information involved (*d*)
- Other means approved by the Director, Division of Facilities and Security (DFS), Office of Administration (ADM) (*e*)

Individuals transporting documents containing SGI shall retain them in their possession at all times, unless they place the documents in the custody of another person authorized access to the information. (ii)

Individuals transporting documents containing other categories of sensitive unclassified information shall retain them in their possession to the maximum extent possible, unless they place the documents in the custody of another person authorized access to the information. Judgment must be used in handling these documents when retention is not feasible. (iii)

Preparation for Transmission (b)

General Rule (i)

- Documents containing sensitive unclassified information must be addressed to an individual authorized access to that information. (*a*)
- Material used for packaging must be opaque and of such strength and durability as to provide secure protection for the document in transit, prevent items from breaking out of the container, and facilitate the detection of any tampering with the container. (*b*)

Safeguards Information (ii)

- Documents containing SGI **may** be hand-carried or transmitted between NRC headquarters facilities by NRC interoffice mail, or between headquarters and regional offices by NRC pouch mail, in a single opaque envelope or wrapper. The envelope or wrapper must have the words "Safeguards Information" at the top and bottom on both sides and be addressed to the intended recipient, with a return address included. (*a*)

Information Originated by NRC, NRC Contractors, or NRC Licensees (A) (continued)

Transmission (6) (continued)

- Whenever documents containing SGI are transmitted outside an NRC facility or an NRC contractor facility by other means or to other destinations, they must be enclosed in two opaque sealed envelopes or similar wrappings. The inner envelope or wrapper must show the address of the intended recipient and the sender on the front and have the words "Safeguards Information" at the top and bottom on both sides. The outer envelope or wrapper must be addressed to the intended recipient, must contain the address of the sender, and must not bear any markings or indication that the document contains sensitive unclassified information. (*b*)

Proprietary Information or Official Use Only Information (iii)

Documents containing Proprietary or Official Use Only information must be transmitted between NRC facilities and outside NRC facilities or NRC contractor facilities in a single opaque envelope or wrapper. The single opaque envelope or wrapper must not bear any markings or indication that the document contains Proprietary or Official Use Only information. Two opaque envelopes or wrappers may be used as described in Section (A)(6)(b)(ii) of this part when the sender believes it necessary to ensure proper handling and protection.

Receipts (iv)

Receipts are not required for sensitive unclassified documents. However, NRC Form 253, "NRC Messenger/Courier Receipt," may be used if the sender wishes to ensure the delivery of the document.

Telecommunications (7)

General Rule (a)

- Utmost discretion must be used in the transmission of any sensitive unclassified information by electrical means. Mail channels are preferable. For further information, refer to Management Directive (MD) 12.4, "NRC Telecommunications Systems Security Program." (i)

Information Originated by NRC, NRC Contractors, or NRC Licensees (A) (continued)

Telecommunications (7) (continued)

- Proprietary and Official Use Only information must be encrypted if encryption is requested by the sender. **Note**: NRC telecommunications from the NRC Secure Communications Center are automatically encrypted and acceptable for transmission of sensitive unclassified information. (ii)
- To request encryption for messages sent through communication centers, the sender shall place the letters "EFTO" (Encrypt For Transmission Only) on the message form between the address and the text of the message. Messages containing SGI, Official Use Only, or Proprietary information must contain the words "SAFEGUARDS INFORMATION," "OFFICIAL USE ONLY," or "PROPRIETARY INFORMATION," as applicable, before the beginning of the text. (iii)

Safeguards Information (b)

SGI must be transmitted over protected telecommunications circuits approved by DFS. Unprotected circuits may be used only under emergency or extraordinary conditions. For the purpose of this requirement, emergency or extraordinary conditions are defined as any circumstances that require immediate communication in order to report, summon assistance for, or respond to a safeguards event or an event that has potential safeguards significance. Examples of these events include—(i)

- Safeguards events that must be reported as specified in 10 CFR 73.71 (i.e., unaccounted-for shipments, suspected thefts, unlawful diversion or radiological sabotage, or events that significantly threaten or lessen the effectiveness of safeguards) (*a*)
- Schedule changes, delays, or equipment breakdowns associated with the transport of spent fuel or Category I strategic special nuclear material (*b*)
- Failure or loss of safety-related equipment identified in the physical security plan as being vital (*c*)

The restriction on telecommunications applies to telephone, telegraph, teletype, communicating word processors, facsimile circuits, and radio (ii)

Information Originated by NRC, NRC Contractors, or NRC Licensees (A) (continued)

Automatic Data Processing (ADP) (8)

SGI and other sensitive data (e.g., personal data, proprietary data, or data that has a high potential for financial loss) may be processed or produced on Information Technology systems, provided that the systems meet the requirements of MD 12.5, "NRC Automated Information Systems Security Program."

Word Processing (9)

SGI and other sensitive data may be processed, stored, or produced on stand-alone personal computers or the NRC Local Area Network provided that the systems meet the criteria of MD 12.5.

Protection of Information During Use (10)

While in use, documents containing sensitive unclassified information must be under the control of an individual authorized access to such information by the individual's division or office director or regional administrator in order to limit access to persons who have a "need-to-know." This requirement is satisfied in the case of SGI if the immediate space in which the documents are held is attended by an authorized individual even though the information is not constantly being used. In the case of Proprietary and Official Use Only information, this requirement is satisfied when the information is not constantly being used by those means that the office or division has determined will prevent unauthorized access. DFS will aid in developing the most practical approach possible.

Storage (11)

Official Use Only and Proprietary Information (a)

Official Use Only and Proprietary information stored in NRC space (headquarters and regional offices) that has electronic access control approved by DFS or NRC contract guards on duty requires no additional physical security measures, unless—

- Specific storage requirements have been published under a Privacy Act system of records. (i)
- The holder deems additional protection (e.g., a locking cabinet) is necessary because of unusual circumstances or the sensitivity of the information (e.g., resident inspection sites). (ii)

Information Originated by NRC, NRC Contractors, or NRC Licensees (A) (continued)

Storage (11) (continued)

Safeguards Information (b)

SGI must be stored in a locked security storage container when unattended or not in actual use. (i)

As the term is used in this part, "security storage container" includes any of the following repositories: (ii)

- A steel filing cabinet equipped with a steel locking bar and a three-position changeable combination, GSA-approved padlock for storage in NRC headquarters and regional office buildings that have sufficient controls to prevent unrestricted access to the container. An NRC office that is occupied by employees during working hours and locked during nonworking hours (cleaning personnel may have keys, if necessary) would be considered to have sufficient access controls. This steel filing cabinet would not be considered adequate for a generally "public" area (e.g., a Public Document Room). (*a*)
- A security filing cabinet that bears a Test Certification Label on the side of the locking drawer, or on an interior plate, and that is marked as a "General Services Administration Approved Security Container." (*b*)
- A bank safe deposit box. (*c*)
- Other repositories that the Director, DFS, judges would provide adequate physical protection. (*d*)

Lock Combinations (c)

The lock combinations protecting any category of sensitive unclassified information must be limited to a minimum number of persons who have a "need-to-know" for operating purposes and are otherwise authorized access to the category of sensitive unclassified information in accordance with the provisions of this part. Combinations must be changed when placed in use, whenever a person having access no longer has an official "need-to-know," or at least once every year.

Information Originated by NRC, NRC Contractors, or NRC Licensees (A) (continued)

Storage (11) (continued)

Inspection of Out-of-Service Storage Repositories (d)

Security storage containers, desks, and other storage repositories to be removed for repair or maintenance, returned to the supplier, or otherwise taken out of service for any reason must be examined to ensure that no classified or sensitive unclassified documents remain therein.

Destruction (12)

Holders of sensitive unclassified information documents are responsible for destroying these documents when they are no longer required. Records of destruction are not required. Documents containing sensitive unclassified information must be destroyed by a method that will prevent reconstruction of the information in whole or in part (see NUREG-0910, "NRC Comprehensive Records Disposition Schedule"). (a)

Documents may be destroyed by tearing them into small pieces (i.e., several pages or documents torn into one-half inch pieces or smaller and thoroughly mixed), or by burning, pulping, pulverizing, shredding, or chemical decomposition. Within NRC headquarters, documents may be placed in receptacles designated for classified waste or receptacles approved by DFS for destruction of sensitive unclassified information. (b)

Removal of Information From the Sensitive Unclassified Category (13)

Necessity for Review (a)

Periodic review of documents containing sensitive unclassified information to determine whether these documents should remain in this category is not required. This review is necessary only when specific circumstances require such action. Typically, a request for the information under the Freedom of Information Act or the Privacy Act would necessitate a review of this type.

Information Originated by NRC, NRC Contractors, or NRC Licensees (A) (continued)

Removal of Information From the Sensitive Unclassified Category (13) (continued)

Who May Remove Information From the Sensitive Unclassified Category (b)

Sensitive Unclassified Information Other Than SGI (i)

The following individuals may remove markings from documents containing sensitive unclassified information (other than SGI) when these individuals determine that the information is no longer in the sensitive unclassified category: (*a*)

- The originator, whose name appears on the document (*1*)
- His or her successor (*2*)
- A supervisor of either of the above (branch chief or above) (see Section (A)(13)(d) of this part) (*3*)

These individuals must be notified if any other persons remove this information from the sensitive unclassified category. (*b*)

SGI (ii)

Any individual authorized to determine that a document contains SGI may remove the marking or indicate that it may be removed whenever the information is no longer in this category, provided that the following individuals are informed: (*a*)

- The individual whose name appears on the document (*1*)
- His or her successor (*2*)
- A supervisor of either of the above (branch chief or above) or other level deemed appropriate by an office director and issued in writing (*3*)

The procedure set forth in Section (A)(13)(d) of this part must be followed. (*b*)

Information Originated by NRC, NRC Contractors, or NRC Licensees (A) (continued)

Removal of Information From the Sensitive Unclassified Category (13) (continued)

Notification (c)

The person authorizing removal of a document from the sensitive unclassified information category or authorizing a change in the category shall so advise, to the extent feasible, the recipients of the document, who in turn shall so advise any subsequent recipient.

Marking (d)

When Information Is Marked (i)

The marking indicating a date or event for removal of the information from the sensitive unclassified category may be placed on documents upon origination or upon removal of the information from the sensitive unclassified category. The person taking the action shall place the following marking on the face of the document: (*a*)

Removed from sensitive unclassified information category (on) or (after)_____

_____	_____	_____	_____
(Signature of person making determination)	(Title)	(Office)	(Date)

The date of cancellation of the marking or the event that will result in cancellation must be indicated. If a date or event is given, any possessor of the information may remove the sensitive unclassified information marking (e.g., "SAFEGUARDS INFORMATION," "OFFICIAL USE ONLY," or "PROPRIETARY INFORMATION") after the date or event has occurred. The last line must be completed with the signature, title, and office of the person authorizing the action and the date of authorization. (*b*)

Information Originated by NRC, NRC Contractors, or NRC Licensees (A) (continued)

Removal of Information From the Sensitive Unclassified Category (13) (continued)

Change in Category (ii)

Documents must be marked to indicate a change of category, the person who is responsible for the change, and the date of the change. For example, if the document is removed from the SGI category but will still contain Official Use Only information, the SGI markings must be removed and the document marked "**OFFICIAL USE ONLY**" and "**LIMITED INTERNAL DISTRIBUTION PERMITTED.**"

Removal of Markings (iii)

As a minimum, the sensitive unclassified information markings on the first page of text and on the outside of the front and back covers, if any, must be blacked out upon removal of a document from the sensitive unclassified information category or upon a change in the category. In the latter case, the new category must be inserted. If there are no covers, the marking must be blacked out or changed on the title page. If there is no title page, the marking must be blacked out or changed on the first page of text and on the outside of the back page. (*a*)

Persons possessing copies of the document, except as stated below, who are advised that the marking is no longer required or that the marking is changed, shall use a marker to **blacken out** or change the sensitive unclassified information markings, as appropriate, on the copies in their possession and indicate on each copy the authority for deleting or changing the markings. (*b*)

Large file rooms and copy distribution centers possessing multiple copies are not required to black out or change the markings but will maintain the notification of removal or change as a record of the action taken. Copies transmitted outside these rooms or centers must be marked to indicate their content. (*c*)

Information Originated by NRC, NRC Contractors, or NRC Licensees (A) (continued)

Removal of Information From the Sensitive Unclassified Category (13) (continued)

Disagreement on Changes of Category (e)

In any instance in which a disagreement exists as to whether a document should be removed from the SGI category, the matter must be referred for final determination to the Director, Division of Fuel Cycle Safety and Safeguards, Office of Nuclear Material Safety and Safeguards, as the contact for issues related to materials and transportation, and to the Director, Division of Inspection Program Management, Office of Nuclear Reactor Regulation, as the contact for issues related to reactors. In other instances of disagreement as to the removal of sensitive unclassified information from a category or a change in the category, the matter should be referred to one of the persons specified in Section (A)(13)(b)(i) of this part.

Information Originated by Sources Other Than NRC, NRC Contractors, or NRC Licensees (B)

General Rule (1)

Sensitive unclassified information, originated by sources other than NRC, NRC contractors, or NRC licensees, must be protected and disseminated under the same security measures set forth in Section (A) of this part for sensitive unclassified information originated by NRC, NRC contractors, or NRC licensees. (a)

Documents originated by sources other than NRC, NRC contractors, or NRC licensees that are marked so as to indicate that they contain sensitive unclassified information (e.g., Company Confidential) must be marked with NRC standard markings to indicate the category of information (e.g., Proprietary information) when the holder determines this marking is necessary for clarification. Holders shall contact the originators of documents in these cases to ensure documents are properly marked. (b)

Information Originated by Sources Other Than NRC, NRC Contractors, or NRC Licensees (B) (continued)

Access (2)

If any doubt exists as to whether it is proper in any particular case to grant access to sensitive unclassified information originating outside NRC, NRC contractors, or NRC licensees, the originating party, or other appropriate person in the agency responsible for the information, or other source from which the information is derived, must be consulted.

Hearings, Conferences, or Discussions (C)

Security Preparations Required for Hearings, Conferences, or Discussions (1)

NRC personnel, NRC consultants, NRC contractor personnel, and others (e.g., bidders) who arrange or participate in hearings, conferences, or discussions (see MD 3.5, "Public Attendance at Certain Meetings Involving the NRC Staff") involving sensitive unclassified information shall—

- Ensure before a hearing, conference, or discussion that participating personnel are identified and are authorized to have access to the information to be discussed (a)
- Indicate to participating personnel that the specific data they will furnish is sensitive unclassified information and advise them of the category of the information (e.g., SGI, Official Use Only, or Proprietary information), together with any protective measures required (b)
- Ensure that no discussion takes place that is audible to persons not authorized access to the information (c)

Where Held (2)

With the exception of inspection exit interviews held at locations owned and controlled by NRC licensees, conferences involving sensitive unclassified information must be held within NRC guarded or controlled areas, if practical. Conferences may be held outside guarded or controlled areas only when the director of a headquarters office or a regional administrator determines that adequate protection can be provided such information.

Protective Orders (D)

Regulations, 10 CFR 2.740(c), for domestic licensing proceedings, provide authority to presiding officers to determine, on motion, whether a trade secret or other confidential research, development, or commercial information will not be disclosed or only will be disclosed in a designated way. This determination is contained in a protective order issued by the presiding officer that sets forth procedures necessary to protect the information.

Exhibit 1

Safeguards Information

The following categories of information and specific items are subject to controls for Safeguards Information (SGI) specified in Part II of this handbook:

- **Physical Protection at Fixed Sites** (A)

  Unclassified information relating to the protection of facilities that possess formula quantities of strategic special nuclear material and power reactors,* specifically—

  - Composite physical security plan for the nuclear facility or site (1)
  - Site-specific drawings, diagrams, sketches, or maps that substantially represent the final design features of the physical protection system (2)
  - Details of alarm system layouts showing location of intrusion detection devices, alarm assessment equipment, alarm system wiring, emergency power sources, and duress alarms (3)
  - Written physical security orders and procedures for members of the security organization, as well as duress codes and patrol schedules (4)
  - Details of the onsite and offsite communications systems that are used for security purposes (5)
  - Lock combinations and mechanical key design (6)
  - Documents and other material that contain lists or locations of certain safety-related equipment explicitly identified in the documents as vital for purposes of physical protection, as contained in physical security plans, safeguards contingency plans, or plant-specific safeguards analyses for production or utilization facilities (7)
  - Composite safeguards contingency plan for the facility or site (8)
  - Those portions of the facility guard qualifications and training plan that disclose features of the physical security system or response procedures (9)
  - Response plans to specific threats detailing size, disposition, response times, and armament of responding forces (10)

* Most of the physical protection information for activities involving a formula quantity of unirradiated strategic special nuclear material would be National Security Information and classified in accordance with the NRC Classification Guide for National Security Information concerning Nuclear Materials and Facilities (CG–NMF–2).

Exhibit 1 (continued)

- **Physical Protection at Fixed Sites** (A) (continued)
  - Size, armament, and disposition of onsite reserve forces (11)
  - Size, identity, armament, and arrival times of offsite forces committed to respond to safeguards emergencies (12)
- **Physical Protection in Transit** (B)

  Unclassified information relating to the protection of shipments of formula quantities of strategic special nuclear material and spent fuel, specifically—
  - Composite transportation physical security plan (1)
  - Schedules and itineraries for specific shipments* (2)
  - Details of vehicle immobilization features, intrusion alarm devices, and communications systems (3)
  - Arrangements with and capabilities of local police response forces, and locations of safe havens (4)
  - Details regarding limitations of radio-telephone communications (5)
  - Procedures for response to safeguards emergencies (6)
- **Inspections, Audits, and Evaluations** (C)

  Unclassified information relating to safeguards inspections and reports, specifically, portions of safeguards inspection reports, evaluations, audits, or investigations that contain details of a licensee's or an applicant's physical security system or that disclose uncorrected defects, weaknesses, or vulnerabilities in the system.**

* Routes and quantities for shipments of spent fuel are not withheld from public disclosure. Schedules for spent fuel shipments may be released 10 days after the last shipment of a current series.

** Information regarding defects, weaknesses, or vulnerabilities may be released after corrections have been made. Reports of investigations may be released after the investigation has been completed, unless withheld pursuant to other authorities, for example, the Freedom of Information Act (5 U.S.C. 552).

Exhibit 2

Information Not Subject to Safeguards Information (SGI) Controls

Certain types of information, even though possibly regarded as SGI, are not subject to the provisions of Part II of this handbook. However, these items may require controls set forth in Part II of this handbook for other categories of sensitive unclassified information.

Most notably, these items include studies, reports, and analyses conducted by or on behalf of the Commission, licensees, or applicants for licenses concerning the safeguarding of nuclear materials or facilities. Information specifically excluded from protection as SGI under Part II of this handbook includes—

- Documents, drawings, or reports submitted by applicants or licensees, or produced by the staff, in response to the environmental and safety requirements contained in 10 CFR Parts 50, 51, 70, and 71 (1)
- Routes and quantities of spent fuel shipments (2)
- Information concerning licensee control and accounting procedures, or inventory differences (not otherwise classified as National Security Information or Restricted Data) for special nuclear material, or source material and byproduct material (3)
- Any information already in the public domain, including commercial safeguards equipment specifications, catalogues, and equipment buying data (4)
- Portions of guard qualification and training plans that do not disclose facility safeguards features or response procedures (5)

Note: Reports to or from the NRC that contain information concerning a licensee's physical protection program for special nuclear material not otherwise designated as SGI or classified as National Security Information or Restricted Data, shall be handled and marked as "PROPRIETARY INFORMATION" as defined by 10 CFR 2.790(d).

Exhibit 3

Safeguards Information Document Marking

SAFEGUARDS INFORMATION

Analysis of
Physical Security Plan
for
Sunshine Nuclear
Power Plant

Violation of protection requirements for SAFEGUARDS INFORMATION subject to CIVIL and CRIMINAL penalties. The determination that this document contains Safeguards information was made by

_____
Name, Title, Organization, Date

SAFEGUARDS INFORMATION

Exhibit 4

Safeguards Information Cover Sheet

NRC FORM 461
(8-89)

U.S. NUCLEAR REGULATORY COMMISSION

SAFEGUARDS INFORMATION

THIS DOCUMENT CONTAINS INFORMATION WHICH MUST BE PROTECTED FROM UNAUTHORIZED DISCLOSURE IN ACCORDANCE WITH NRC REGULATIONS. NRC MANUAL CHAPTER AND APPENDIX 2101; 10 CFR 73.21; AND SECTION 147, ATOMIC ENERGY ACT OF 1954, AS AMENDED, APPLY. VIOLATIONS ARE SUBJECT TO CIVIL OR CRIMINAL PENALTIES.

THIS DOCUMENT IS NOT TO BE LEFT UNATTENDED OR ACCESSIBLE TO UNAUTHORIZED PERSONS. WHEN NOT IN USE, IT MUST BE STORED IN A LOCKED SECURITY STORAGE CONTAINER.

IT IS YOUR RESPONSIBILITY TO PROTECT THE INFORMATION CONTAINED IN THIS DOCUMENT FROM COMPROMISE, THEFT OR UNAUTHORIZED DISCLOSURE.

SAFEGUARDS INFORMATION

Exhibit 5

Proprietary Information Cover Sheet

NRC FORM 190
(9-1999)
NRCMD 3.12

U.S. NUCLEAR REGULATORY COMMISSION

PROPRIETARY INFORMATION

NOTICE

THE ATTACHED DOCUMENT CONTAINS OR IS CLAIMED TO CONTAIN PROPRIETARY INFORMATION AND SHOULD BE HANDLED AS NRC SENSITIVE UNCLASSIFIED INFORMATION. IT SHOULD NOT BE DISCUSSED OR MADE AVAILABLE TO ANY PERSON NOT REQUIRING SUCH INFORMATION IN THE CONDUCT OF OFFICIAL BUSINESS AND SHOULD BE STORED, TRANSFERRED, AND DISPOSED OF BY EACH RECIPIENT IN A MANNER WHICH WILL ASSURE THAT ITS CONTENTS ARE NOT MADE AVAILABLE TO UNAUTHORIZED PERSONS.

COPY NO. _____

DOCKET NO. _____

CONTROL NO. _____

REPORT NO. _____

REC'D W/LTR DTD. _____

PROPRIETARY INFORMATION

Exhibit 6

Official Use Only Information Cover Sheet

THIS IS A COVER SHEET

OFFICIAL USE ONLY

PROCEDURES FOR HANDLING "OFFICIAL USE ONLY" INFORMATION ARE AVAILABLE IN MANAGEMENT DIRECTIVE 12.6

NRC FORM 190B (9-1999) NRCMD 12.6 THIS IS A COVER SHEET U.S. NUCLEAR REGULATORY COMMISSION