

TN: DT-05-20

To: NRC Management Directives Custodians

Subject: Transmittal of Management Directive 12.2, "NRC Classified Information Security Program"

Purpose: Directive and Handbook 12.2 are being revised to reflect the changes in Executive Order 12958, as amended; to include the creation of the Office of Nuclear Security and Incident Response (NSIR); to reflect the transfer of responsibilities of NRC's Classified Information Security Program from the Office of Administration to NSIR; and to designate the Deputy Executive Director for Reactor and Preparedness Programs as the Senior Agency Official.

Office and
Division of Origin: Office of Nuclear Security and Incident Response
Division of Nuclear Security

Contact: Rhonda Bethea, 301-415-2254

Date Approved: April 27, 1999 (**Revised: December 6, 2005**)

Volume: 12 Security

Directive: 12.2, "NRC Classified Information Security Program"

Availability: Rules and Directives Branch
Office of Administration
Michael T. Lesar, 301-415-7163
Christy Moore, 301-415-7086

NRC Classified
Information Security
Program

Directive
12.2

Contents

Policy	1
Objectives	1
Organizational Responsibilities and	
Delegations of Authority	1
Chairman	1
Commission	2
Inspector General (IG)	2
Secretary of the Commission (SECY)	3
Executive Director for Operations (EDO)	3
Deputy Executive Director for Reactor and Preparedness Programs (DEDR)	3
Deputy Executive Director for Information Services and Administration, and Chief Information Officer (DEDIA)	4
Office of the General Counsel	5
Director, Office of International Programs (OIP)	5
Director, Office of Nuclear Security and Incident Response (NSIR)	5
Office Directors and Regional Administrators	5
Director, Division of Nuclear Security (DNS), NSIR	6
Director, Division of Facilities and Security (DFS), Office of Administration (ADM)	7
Applicability	8
Handbook	8
Exceptions or Deviations	8
References	8



U. S. Nuclear Regulatory Commission

Volume: 12 Security

NSIR

NRC Classified Information Security Program Directive 12.2

Policy (12.2-01)

It is the policy of the U.S. Nuclear Regulatory Commission 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.

Objectives (12.2-02)

To ensure that all NRC personnel responsible for safeguarding classified information (National Security Information [NSI], Restricted Data [RD], and Formerly Restricted Data [FRD]) and activities involving this information shall adhere to the procedures in this directive and handbook.

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)

Approved: April 27, 1999

(Revised: December 6, 2005)

Organizational Responsibilities and
Delegations of Authority
(12.2-03) (continued)

Chairman
(031) (continued)

- Designates, if required, NRC and other personnel authorized original Secret or Confidential classification authority. This authority may be delegated. (b)

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 (E.O.) 12958, as amended, 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)

Inspector General (IG)
(033)

As delegated by the Chairman, has original Secret classification authority.

Organizational Responsibilities and
Delegations of Authority
(12.2-03) (continued)

Secretary of the Commission (SECY)
(034)

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

Executive Director for Operations (EDO)
(035)

- As delegated by the Chairman, has original Top Secret classification authority. (a)
- As assigned by the Chairman, is responsible for delegating original classification authority at the Secret and Confidential levels to NRC employees. (b)
- Authorizes access to classified NSCI for NRC Commission and staff personnel with a "Q" clearance. (c)

Deputy Executive Director for
Reactor and Preparedness
Programs (DEDR)
(036)

- As the Senior Agency Official who directs and administers the agency's program under which information is classified, safeguarded, and declassified, actively oversees implementation of E.O. 12958, as amended, by NRC, NRC contractors, NRC licensees, and licensee-related organizations. (a)
- Designates original classifying authority at Secret and Confidential levels to NRC personnel, except for those officials designated in Commission-level offices. (b)

Organizational Responsibilities and
Delegations of Authority
(12.2-03) (continued)

Deputy Executive Director for
Reactor and Preparedness
Programs (DEDR)
(036) (continued)

- Approves classification guides, except those requiring Commission approval. (c)
- Issues and maintains guidelines for systematic review for declassification of 25-year-old NSI 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. (d)
- Approves the designation of NRC personnel authorized to declassify or downgrade NSI. (e)
- Acts on appeals for denial of information requested under the mandatory review procedures of E.O. 12958, as amended, when the request involves information generated by offices and regions reporting to the EDO. (f)

Deputy Executive Director for Information
Services and Administration, and Chief
Information Officer (DEDIA)
(037)

Approves plans for the protection of classified information in an emergency.

Organizational Responsibilities and
Delegations of Authority
(12.2-03) (continued)

Office of the General Counsel (OGC)
(038)

Reviews any concerns regarding the legal aspects of NRC transfer of information to foreign governments or international organizations.

Director, Office of International
Programs (OIP)
(039)

- 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 Nuclear Security
And Incident Response (NSIR)
(0310)

- Provides overall NRC information security program guidance and direction. (a)
- Provides mandatory Web-based Security Awareness training to be completed annually by all NRC employees. (b)

Office Directors and
Regional Administrators
(0311)

- 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)

Organizational Responsibilities and
Delegations of Authority
(12.2-03) (continued)

Office Directors and
Regional Administrators
(0311) (continued)

- Advise the Division of Nuclear Security (DNS), NSIR, and the Division of Facilities and Security (DFS), Office of Administration (ADM), of any existing or proposed classified activities in organizations under their jurisdiction. Report any significant change or termination of classified activities to DNS/DFS for review of associated contracts, subcontracts, or similar actions. (b)
- Furnish security plans to DNS/NSIR and DFS/ADM, as appropriate. (c)
- Advise DNS and 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 Nuclear
Security (DNS), NSIR
(0312)

- Plans, develops, establishes, and administers policies, standards, and procedures for the NRC classified information

Organizational Responsibilities and
Delegations of Authority
(12.2-03) (continued)

Director, Division of Nuclear
Security (DNS), NSIR
(0312) (continued)

security program, including management of the security classification program. (a)

- Coordinates the security aspects of the disclosure of classified information to foreign governments and international organizations. (b)
- Renders foreign ownership, control, or influence (FOCI) determinations and facility security clearances for licensees. (c)

Director, Division of Facilities
And Security (DFS), Office of
Administration (ADM)
(0313)

- Provides physical security requirements and procedures to protect classified information, sensitive unclassified information, and facilities and NRC assets. (a)
- Administers the visitor control program, which covers visits requiring access to classified information. (b)
- Investigates and determines the eligibility of individuals for NRC access authorization and/or employment clearance. (c)
- Provides facility security clearances for NRC contractors. (d)

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)

NSIR 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 Chairman, the Commission, or the DEDH 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)

Central Intelligence Agency

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

Code of Federal Regulations—

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

References

(12.2-07) (continued)

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."

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

10 CFR Part 1045, "Nuclear Classification and Declassification."

Executive Orders—

Executive Order (E.O.) 12333, "United States Intelligence Activities," December 4, 1981.

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

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

References

(12.2-07) (continued)

E.O. 12968, "Access to Classified Information," August 2, 1995.

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

National Security Decision Directives

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

National Security Decision Directive 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.

Nuclear Regulatory Commission

NRC Management Directives—

3.1, "Freedom of Information Act."

3.2, "Privacy Act."

3.4, "Release of Information to the Public."

5.5, "Public Affairs Program."

12.1, "NRC Facility Security Program."

12.3, "NRC Personnel Security Program."

12.4, "NRC Telecommunications Systems Security Program."

References

(12.2-07) (continued)

12.5, "NRC Automated Information Security Program."

12.6, "NRC Sensitive Unclassified Information Security Program."

NUREG-0910, "NRC Comprehensive Records Disposition Schedule" (March 1998).

Presidential Directive

"Basic Policy Governing the Release of Classified Defense Information to Foreign Governments," September 23, 1958.

United States Code

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

Crimes and Criminal Proceedings, Title 18 U.S.C.

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

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

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)	9
Marking Classified Documents (3)	14
Change of Classification and Marking (4)	19
Declassification of National Security Information (5)	25
Deletion of Classified Information From Documents (6)	29
Markings for Specific Types of Classified Information (7)	31
Record Classification Actions (RCA) System (8)	36
Control of Secret and Confidential Documents (C)	37
Cover Sheets (1)	37
Assurances Required Before Transmission of Classified Information (2)	37
Means of Transmission of Secret Documents Inside the United States (3)	38
Means of Transmission of Secret Documents Outside the United States (4)	39
Means of Transmission of Confidential Documents Inside and Outside the United States (5)	40
Electronically Transmitted Classified Messages (6)	41
Transmission of Documents From Other Agencies (7)	43
Preparation of Secret and Confidential Documents for Transmission (8)	43
Classified Documents From Other Agencies (9)	46
Destruction of Secret and Confidential Documents (10)	47
Loss or Possible Compromise of Classified Information (11)	48
Classification Guides (D)	48
Types of Guides (1)	49
Approval of Guides (2)	49
Review of Guides (3)	49
Dissemination of Guides (4)	50
Content of Guides (5)	50

Contents (continued)

Classification Appraisals (E)	50
Frequency of Appraisals (1)	51
Reports (2)	51
Foreign Ownership, Control, or Influence (FOCI) (F)	52

Part II

Special Handling of Classified Information	55
Control of Top Secret Documents (A)	55
Access Lists (1)	55
Sanctions (2)	55
Central Top Secret Control Officer and Top Secret Control Officers (3)	56
Accountability Control Files (4)	58
Assignment of a Control Number to Documents From Other Agencies (5)	59
Physical Inventory (6)	59
Reproduction of Top Secret Documents (7)	61
Reproduction of Top Secret Documents From Other Agencies (8)	62
Transmission of Top Secret Documents (9)	62
Receipts (10)	63
Destruction of Top Secret Documents (11)	64
Naval Nuclear Propulsion Information (B)	64
National Security Council Information (NSCI) (C)	65
Responsibilities (1)	65
Access Lists (2)	66
Requirements (3)	67
Transfer of Classified Information to Foreign Governments and International Organizations (D)	70
Authorities (1)	70
Criteria (2)	71
Responsibilities (3)	73
Internal Procedures (4)	75
Classified Conferences (E)	81
Conferences and Symposia (1)	81
Publication or Release of Documents (2)	82

Contents (continued)

Review of Documents (3)	82
Review of Documents Submitted by Uncleared Authors (4)	82
Review of Documents Submitted by Formerly Cleared Persons or by Authors With Active Clearances (5)	83
Hand-carrying Classified Material (F)	83
Courier Letters (1)	83
Courier Card (2)	83
Transporting Classified Material by Commercial Airlines (G)	84
 Exhibits	
1 Required Markings for Classified Documents	87
2 Declassification Markings	88
3 Subject or Title Marking and Portion-Marking	89
4 Upgrading, Downgrading, and Transclassification Markings	90
5 Deleting Classified Information From Classified Documents	91
6 Required Markings for an Unclassified Transmittal Document	92
7 Required Markings for a Classified Transmittal Document	93
8 Required Markings for Envelopes or Wrappers	94
9 Foreign Equivalent Markings	95

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., E.O. 12958, "Classified National Security Information," as amended); and other directives (e.g., directives of the Information Security Oversight Office (ISOO) and the 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)

All personnel are personally and individually responsible for providing proper protection of classified information in their custody and control. Any NRC employee who finds classified information unprotected should take control of it and immediately contact the Division of Facilities and Security (DFS) for guidance.

Classification Determinations (a)

Classification determinations regarding NRC information must be made solely by NRC authorized classifiers, including NRC

Classification (B) (continued)

Responsibilities To Protect Classified Information (1)
(continued)

contractors who have been delegated that authority and trained to exercise the authority. Authorized classifiers are delegated either original or derivative classification authority. (i)

An authorized classifier with original classification authority may classify information, on the basis of his or her knowledge, authority, and expertise, and if it meets the following criterion— (ii)

The information is owned by, produced by or for, or is under the control of the United States Government and meets the requirements outlined in E.O. 12958, as amended, Section 1.4(a)-(h).

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). The AEA constitutes the authority for classification of Restricted Data (RD) and Formerly Restricted Data (FRD). Because the AEA classifies this information at its inception, all these classification determinations are derivative. (iii)

Each official with original classification authority also possesses derivative classification authority. (iv)

In an emergency, when necessary to respond to an imminent threat to life or in defense of the homeland, the Chairman or any designee may authorize the disclosure of classified information to an individual or individuals who are otherwise not eligible for access, in accordance with Section 4.2(b) of E.O. 12958, as amended. (v)

Classification (B) (continued)

Responsibilities To Protect Classified Information (1)
(continued)

Delegation of Classification Authority (b)

A *Federal Register* notice of March 28, 2003, designates the Chairman of NRC as a Top Secret original classification authority under E.O. 12958, as amended, Section 1.3. As authorized, the Chairman has delegated original classification authority to the four Commissioners, the Executive Director for Operations (EDO), the Deputy Executive Director for Reactor and Preparedness Programs (DEDR), and the Inspector General (IG). The Chairman also has assigned the EDO and the DEDH responsibility for delegating original classification authority at the Secret and Confidential levels to NRC personnel. Original classification authority cannot be delegated to NRC contractors. The responsibility for delegating derivative classification authority to NRC personnel, NRC contractor personnel, and other personnel has been assigned by the DEDR to the Director of the Division of Nuclear Security (DNS), Office of Nuclear Security and Incident Response (NSIR). (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 of DNS. These requests must include— (ii)

- Names and positions of the individuals for whom authority is sought (a)
- 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 of DNS will evaluate the request and take the necessary

Classification (B) (continued)

Responsibilities To Protect Classified Information (1)
(continued)

action to approve or disapprove it, or have the DEDH approve or disapprove a request for original classification authority. (iii)

Authorized Classifier Training (c)

All authorized classifiers must be trained before they exercise their authority. The Information Security Section (INFOSEC) of DNS/NSIR conducts classifier training when an individual is delegated classification authority. (i)

INFOSEC will provide training materials to those classifiers, original or derivative, in the regional offices. This training must be completed before classifiers exercise their authority. (ii)

Responsibilities of Authorized Classifiers (d)

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

Original classification authorities must receive training in original classification that includes instruction on the proper safeguarding of classified information and of criminal, civil, and administrative sanctions that may be brought against an individual who fails to protect classified information from unauthorized disclosures. (ii)

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— (iii)

- Identified in a classification guide (a)

Classification (B) (continued)

Responsibilities To Protect Classified Information (1)
(continued)

- 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— (*iv*)

- 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*)

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— (*v*)

- 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 DNS for a determination. When

Classification (B) (continued)

Responsibilities To Protect Classified Information (1)
(continued)

there is reasonable doubt about the need to classify information or the appropriate classification level, the following actions must be taken— (vi)

- 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, for example, RD, 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. (vii)

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

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. (ix)

Responsibilities of Originators (e)

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

Classification (B) (continued)

Responsibilities To Protect Classified Information (1)
(continued)

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)

"No Comment Policy" for Classified Information (f)

Occasionally, statements may appear in the public domain (e.g., newspapers) that contain classified information. The fact that specific classified information appears is itself protected at the same level as the information in question within Government channels. In addition, the fact that the information appeared publicly does not make it unclassified information. It is NRC policy to neither confirm nor deny that information appearing in the public domain is or is not classified information. Any questions raised about the accuracy, sensitivity, or technical merit of such information should be responded to in a "no comment" manner.

Classification Challenges (g)

Persons who are in authorized possession of classified National Security Information (NSI) and who in good faith believe that the classification level of the information is too high for its content (overclassification) or too low for its content (underclassification) 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

Classification (B) (continued)

Responsibilities To Protect Classified Information (1)
(continued)

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, DNS/NSIR, for assistance. (b)
- Persons who challenge classification decisions have the right to appeal the decision to the Interagency Security Classification Appeals Panel (ISCAP). The ISCAP was created by the President under Section 5.3 of E.O. 12958, as amended, to decide on appeals by authorized persons who have filed classification challenges under Section 1.8 of E.O. 12958, as amended. INFOSEC, DNS, 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)
- The agency shall provide an initial written response to a challenge within 60 days. If the agency is unable to respond within 60 days, the agency must acknowledge the challenge in writing and provide a date by which the agency will respond. If the agency does not respond within 120 days, the challenger has the right to forward the challenge to the ISCAP for a decision. (e)

Persons who are in authorized possession of an RD or FRD document and who in good faith believe that the classification level of the information is improper are encouraged and expected to challenge the classification with the RD classifier who classified the document as stated in 10 CFR 1045.39. (iii)

Classification (B) (continued)

Responsibilities To Protect Classified Information (1)
(continued)

Limitations on Classification (h)

In accordance with Section 1.7 of E.O. 12958, as amended, 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 needs protection 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.

Classification (B) (continued)

Classification of Protected Information (2) (continued)

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 (NSI) (i)

Information may not be considered for classification as NSI unless it concerns—(a)

- Military plans, weapons systems, or operations (1)
- 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, which includes defense against transnational terrorism (5)
- U.S. Government programs for safeguarding nuclear materials or facilities (6)
- The vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to national security, which includes defense against transnational terrorism (7)
- Weapons of mass destruction (8)

Classification (B) (continued)

Classification of Protected Information (2) (continued)

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. This practice is known as classification by compilation. (b)

NSI 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 (RD) and Formerly Restricted Data (FRD) (ii)

The AEA is the basis for the determination that all RD and FRD are classified. Section II of the AEA defines RD and Section 142 establishes the basis for the concept of FRD. All RD and FRD classification actions are derived from the AEA. Current classification guidance conveys the types of information that must be designated as RD and FRD and the classification level that must be assigned to the information. This classification guidance may be obtained from INFOSEC, DNS/NSIR.

Levels of Classification (c)

The three levels of classification for the protection of both NSI and RD are “Top Secret,” “Secret,” and “Confidential.” Only these three classification designators may be used to identify the level of classification assigned to information.

A Special Access Program is established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level. The number of persons who have access to this information is reasonably small and commensurate

Classification (B) (continued)

Classification of Protected Information (2) (continued)

with the objective of providing enhanced protection for the information involved.

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. Unauthorized disclosure of Confidential information is presumed to cause damage to the National Security, Secret disclosure presumes serious damage, and Top Secret disclosure presumes exceptionally grave damage.

Classification Authority (ii)

The classification authority for NSI is the authorized original classifier, a classification guide, or a source document. The classification authority for RD or FRD is the AEA, as conveyed by classification guides.

Duration of Classification (iii)

The duration of classification is the length of time the information must remain classified. For original classifications, NSI must be classified in accordance with E.O. 12958, as amended. 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 unless the original classification authority determines the sensitivity of the information requires that it shall be marked for declassification 25 years from the date of the original decision.

Classification (B) (continued)

Classification of Protected Information (2) (continued)

Records of permanent historical value should be classified under E.O. 12958, as amended, Section 3.3.

Declassification Exemptions (iv)

NSI 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 E.O. 12958, as amended, Section 3.3(b). Normally, exemption from declassification may not exceed 25 years.

Classification Extensions (v)

If NSI 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, change the level of classification, or reclassify specific information only when the standards and procedures for classifying information under E.O. 12958, as amended, are followed. An original classification authority may extend the duration of classification for information contained in nonpermanent records beyond 25 years in accordance with the standards and procedures for classifying information. Except for information that identifies a confidential human source or a human intelligence source, all other information shall identify a specific date or event for declassification.

Information Classified Under Previous Executive Orders (vi)

NSI marked "Originating Agency's Determination Required" (OADR) under previous Executive Orders may be declassified if the information is declassifiable under E.O. 12958, as amended. The information may be re-marked to establish a duration of classification consistent with the requirements of E.O. 12958, as amended, or if the information is of permanent historical value, it

Classification (B) (continued)

Classification of Protected Information (2) (continued)

may remain classified for 25 years from the date of original classification when it is automatically declassified in accordance with E.O. 12958, as amended, Section 3.3.

Restricted Data and Formerly Restricted Data Exemption (vii)

RD and FRD are exempt from automatic declassification. AEA Sections 141 and 142 set forth the policy regarding review and declassification of RD and transfer of information from the RD category to the FRD status. See Section (B)(4) of this part for declassification of NSI, RD, and FRD.

Marking Classified Documents (3)

Portion-Marking (a)

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 NSI must be marked. Documents containing RD or FRD are not portion 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

Classification (B) (continued)

Marking Classified Documents (3) (continued)

(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

(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, for example, "The entire text is classified at the same level, in conjunction with the page marking." (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 of DNS, who will evaluate and make the appropriate recommendation to ISOO. (ii)

Classification (B) (continued)

Marking Classified Documents (3) (continued)

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 highest overall classification level of the entire document must be placed at the top and bottom of each page. However, for RD, classifiers shall ensure that documents containing RD and FRD 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). (iii)

Category of Classified Information (b)

The category markings for RD or FRD must be placed on the lower left side of the document. The category marking for NSI need not be placed on the document.

Classification Markings for National Security Information (c)

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

Classified By: David Smith, Chief, ABC Branch

Reason: (Cite reason from E.O. 12958, as amended, Section 1.4)

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

Classification (B) (continued)

Marking Classified Documents (3) (continued)

An example of a derivative classification marking follows:

Derived From: Classification Guide/Date

Reason: (Cite reason from E.O. 12958, as amended, Section 1.4)

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

Classifier: Jane Jones, Chief, XYZ Branch

If a classifier cannot determine an earlier specific date or event for declassification, NSI shall be marked for declassification 10 years from the date of the original decision. (ii)

If it is determined that NSI must remain classified longer than 10 years, the original classifier must cite a date that is 25 years from the date of original classification under E.O. 12958, as amended, Section 1.4. (iii)

Reclassification of Information (d)

If it is determined that NSI must be reclassified after being declassified and released to the public, the action is taken in writing by the Chairman of NRC as identified in E.O. 12958, as amended, Section 1.7. For example—

This document has been reclassified in accordance with E.O.12958, as amended, Section 1.7, by authority of the Chairman of NRC.

Signed and dated

Classification (B) (continued)

Marking Classified Documents (3) (continued)

Classification Markings for Restricted Data (e)

RD will not have the same classification markings as NSI. RD is never subject to automatic declassification. 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 document contains Restricted Data as defined in the Atomic Energy Act of 1954. Unauthorized disclosure is subject to Administrative and Criminal sanctions.

In addition, the source and classifier of RD must be identified by the following marking: (ii)

Classified By: Classification Guide ABC (if the guide is unavailable, a source document may be used)

Derivative Classifier: _____
(Name and Title)

Classification Authority (f)

The classification authority for NSI is the authorized classifier, the classification guide, or the source document. If a document is classified on the basis of more than one source document or classification guide, the phrase “Multiple Sources” must be cited as 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 RD and FRD is the authorized derivative classifier. Original classification authority for RD lies with the Department of Energy (DOE) under the AEA. NRC may not make original classification decisions for RD. (ii)

Classification (B) (continued)

Marking Classified Documents (3) (continued)

Declassification Markings (g)

NSI may be declassified by the originator, his or her successor, their supervisor, or by an individual so designated by the Director of DNS. RD may be declassified by persons appointed by DOE. (i)

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

This document has been declassified under the provisions of E.O. 12958, as amended, dated March 28, 2003.

By Authority of _____
(Declassification Authority)

Date of Declassification _____

Change of Classification and Marking (4)

Upgrading (a)

A notice that a document containing NSI was mistakenly issued as unclassified or was mistakenly declassified must be classified and marked at an appropriate level, but not lower than Confidential. A notice that a document containing RD 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)

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

Classification (B) (continued)

Change of Classification and Marking (4) (continued)

- 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 of the Information and Records Services Division, Office of Information Services (OIS); the Chief of the Security Branch, DFS, Office of Administration (ADM); and all known holders of the document, as determined by DNS. (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 accounted for and re-marked or destroyed, the notice may 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)

Classification (B) (continued)

Change of Classification and Marking (4) (continued)

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

Re-marking 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 to 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)

NSI 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 of DNS and the Chief of INFOSEC have been delegated downgrading authority. (i)

Classification (B) (continued)

Change of Classification and Marking (4) (continued)

DNS should be consulted for downgrading instructions. RD and FRD 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 classified document shall notify all known holders of the document. (iii)

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, if any (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)

Classification (B) (continued)

Change of Classification and Marking (4) (continued)

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 to be marked out and replaced with the new downgraded classification. (vi)

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. (vii)

Classification changed to: (insert new level)

By authority of: (person authorizing change)

By: (signature of person making change)

Date: (date of change)

RD and FRD are exempt from automatic downgrading. NSI 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

Classification (B) (continued)

Change of Classification and Marking (4) (continued)

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. (viii)

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 of DNS. (ix)

Transclassification (c)

“Transclassification” is the transfer of information from the RD category to the FRD 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 of DNS. Contact DNS when necessary to transclassify information. (i)

Upon receipt of a transclassification notice, the person responsible for the transclassification shall cross out the existing RD 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)

Category changed to: (insert new category)

By authority of: (person authorizing change)

By: (signature of person making change)

Date: (Date of change)

Classification (B) (continued)

Declassification of National Security Information (5)

Authorities (a)

NSI 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 of DNS or the Chief of INFOSEC. (i)

RD and FRD 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 of DNS, who will coordinate the matter with other affected agencies, as necessary. (ii)

Automatic Declassification (b)

NSI 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 E.O. 12958, as amended. (i)

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

- Reveal the identity of a confidential human source, or human intelligence source, or reveal information regarding intelligence sources or methods (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*)
- Reveal information, including foreign government information, that would clearly and demonstrably impair U.S. foreign relations (*e*)
- Clearly impair the U.S. Government's ability to protect the President, the Vice President, or other officials (*f*)
- Clearly and demonstrably impair national preparedness plans (*g*)
- Seriously and demonstrably impair current national security emergency preparedness plans or reveal current vulnerabilities of systems, installations, or projects relating to the national security (*h*)
- Violate a statute, a treaty, or an international agreement (*i*)

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

At least 180 days before information is automatically declassified under Section 3.3 of E.O. 12958, as amended, the Senior Agency Official shall notify the Director of the Information Security Oversight Office of any specific information beyond that included above that the agency proposes to exempt from automatic declassification. (iv)

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 the Director of DNS.

Classification (B) (continued)

Declassification of National Security Information (5)
(continued)

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 from other Government agencies to review documents for declassification. Information is subject to review for declassification under several circumstances, a request (e.g., under the Freedom of Information Act [FOIA]), a mandatory review, or a systematic review. In these cases, a request for declassification of NSI 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 of DNS. RD and FRD will be declassified in accordance with the provisions of Section (B)(2)(c)(vii) of this part.

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

Declassification reviews and other actions involving review of classified information in accordance with the FOIA or the Privacy Act (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 of DNS 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)

If NRC receives an FOIA or a PA request for records in its possession that were classified by another agency, 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. When the

Classification (B) (continued)

Declassification of National Security Information (5)
(continued)

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 E.O. 12958, as amended, or earlier Executive Orders is subject to a review for declassification under provisions of E.O. 12958, as amended, Section 3.5. 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 DNS upon request.

Systematic Review for Declassification (iv)

All NRC classified information is subject to systematic review for declassification under the provisions of E.O. 12958, as amended, Section 3.4. All such declassification reviews will be conducted in accordance with the NRC systematic review guidelines, which are available from DNS upon request. As stated in Section 5.2(b) of E.O. 12958, as amended, the Director of ISOO will review and approve implementing regulations and agency guides for systematic declassification review before issuance by NRC.

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

Classification (B) (continued)

Declassification of National Security Information (5)
(continued)

Director of DNS, 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 of DNS. (b)
- Contents of the Notice. Declassification notices must identify the document as fully as possible, stating the title, the 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 E.O. 12958, as amended, Section 3.5, a notification is not necessary because these documents are official record copies that are released to the Agencywide Documents Access and Management System (ADAMS) after declassification. (d)

Deletion of Classified Information From Documents (6)

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

Classification (B) (continued)

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

Care must be exercised to ensure that classified information is no longer discernable from any copies. Under no circumstances will the original copy of the document be redacted; only copies may be redacted. (b)

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

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, the title page, the first and the last page of text, and the outside back cover need to be crossed out. Note: all classified information must be removed from each page. (d)

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

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)

Classification (B) (continued)

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 must have the same classification marking. (a)

The lower right side of the first page of the transmittal must be marked to indicate the level of information contained in the transmittal letter when standing alone; for example, when separated from the classified enclosure, this transmittal is unclassified. Additionally, if the information is RD, the lower left side of the first page of the transmittal document must be marked to identify it as transmitting RD. (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):

- 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)

Classification (B) (continued)

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

- 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 NSI and the other document(s) being transmitted is (are) RD/FRD, the lower left side of the transmittal must also be marked "RD/FRD" 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 existing information from several sources must be treated as a new document and classified and marked in accordance with Sections (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

Classification (B) (continued)

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

highest level of classification contained therein or, if warranted by compilation, a higher classification level.

Drafts and Working Copies (b)

Drafts and working copies of documents that contain classified information must be marked with the appropriate classification level and RD category marking if the draft contains RD in accordance with Section (B)(3)(b) 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. Drafts retained for 180 days or longer must be marked to include all classification and declassification information. In these instances, the document must be classified and entered into the automated record classification actions (RCA) system in accordance with Section (B)(8) of this part. (ii)

Top Secret documents must be documented in accordance with Part II(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:

Classification (B) (continued)

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

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 U.S. classification level that will ensure a degree of protection at least equivalent to that required by the entity that furnished the information (see Exhibit 9 for "Foreign Equivalent Markings"). 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)

Documents originated by NRC that contain foreign government information must be marked in accordance with Section (B)(3) of this part and, if applicable, assigned a U.S. classification level that will ensure a degree of protection at least equal to that afforded equivalent U.S. information. 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 U.S. origin. (iii)

Classification (B) (continued)

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

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)(a) of this part must be parenthetically placed after the name of each document. (c)

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

Translations (f)

Translations of U.S. 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).

Classification (B) (continued)

Record Classification Actions (RCA) System (8)

The RCA system is an automated system that allows authorized classifiers to record information about each classification decision that they make. It 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 on the desktop of each authorized classifier's personal computer following his or her designation and training as a classifier. Upon receiving training, each classifier will be given a unique number that will allow the classifier to log onto the RCA system. This automated record 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 DNS by the authorized original or derivative classifier authorizing a classification, downgrading, or declassification action, excluding automatic downgrading or declassification only if access to the online system is not available. The authorized classifier submits the original and one copy of NRC Form 790 to DNS and retains one copy for his or her files. DNS will monitor all data index input and maintain the system's records. (b)

DNS 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 as required. The RCA system enables DNS 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 (both available in the NRC Supply Store), 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. Appropriate marking instructions and selected handling procedures can be found on the reverse side of the cover sheets. 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 protecting 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. Authority for NRC or NRC contractor employees to hand-carry classified documents within the continental United States must be granted by the Director of DNS. (b)

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

Assurances Required Before Transmission of Classified Information (2) (continued)

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, "NRC Facility Security Program," for storage of classified documents). (d)

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

Means of Transmission of Secret Documents Inside the United States (3)

Persons hand-carrying Secret documents shall keep the documents continuously in their possession until the documents are stored in an approved facility. A courier letter or a courier card approved by the Director of DNS is required when hand-carrying classified information (see Sections II(F)(1) and (2) for more details). (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 in accordance with Section II (A)(9) of this handbook (i)

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

**Means of Transmission of Secret Documents Inside the
United States (3) (continued)**

- 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 (ii)
- A cleared commercial carrier or a cleared commercial messenger service engaged in intracity/local delivery of classified mail (iii)
- 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.) (iv)

**Means of Transmission of Secret Documents Outside the
United States (4)**

- U.S. Postal Service registered mail through Army, Navy, or Air Force postal service facilities. (This method must have prior approval from the Director of DFS and assurance that the information will not pass out of control of U.S. citizens or through a foreign postal system. This method may be used to transmit Secret documents to and from the U.S. Government or its contractor employees or members of the Armed Forces in a foreign country.) (a)
- Department of State diplomatic pouch. (Documents may be transmitted to U.S. 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 of DNS before

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

**Means of Transmission of Secret Documents Outside the
United States (4) (continued)**

it is used. The approval may be granted for individual transmissions or on a blanket basis.) (b)

- An authorized person hand-carrying Secret documents to and from foreign countries. (The approval of the Director of DNS 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.) (c)

**Means of Transmission of Confidential Documents Inside and
Outside the United States (5)**

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 courier letter or a courier card approved by the Director of DNS is required when hand-carrying classified information (see Sections II(F)(1) and (2) for more details).(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)

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

Means of Transmission of Confidential Documents Inside and Outside the United States (5) (continued)

- 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)

Electronically Transmitted Classified Messages (6)

Classified messages must be transmitted only by electronic means that are protected with NSA-approved encryption and that have been approved by DNS and OIS. Transmission of classified information in ADAMS or in the Electronic Information Exchange is prohibited. 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 electronically 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)(a) of this part. (d)

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

Electronically Transmitted Classified Messages (6) (continued)

The last line of text of a classified message containing NSI 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, if so requested. (iii)
- Destroy all copies of classified messages in the center's possession 90 days after transmission unless a longer period is approved by the Director of DNS. (iv)

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)

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

Electronically Transmitted Classified Messages (6) (continued)

- 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 of DNS. (iii)
- Maintain records of the destruction of all Top Secret messages. (iv)

Transmission of Documents From Other Agencies (7)

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

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

Preparation of Secret and Confidential Documents for Transmission (8)

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.

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

**Preparation of Secret and Confidential Documents for
Transmission (8) (continued)**

Preparation of Receipts (a)

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

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" (available on InForms), 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 should be sealed (e.g., seams taped) so as to indicate whether or not the envelope has been opened or otherwise tampered with. (a)

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

**Preparation of Secret and Confidential Documents for
Transmission (8) (continued)**

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. (*b*)

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. (*c*)

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

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*)

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

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

**Preparation of Secret and Confidential Documents for
Transmission (8) (continued)**

notify DFS, DNS, 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 (9)

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 E.O. 12958, as amended). No exceptions to this rule are permitted unless coordinated, in advance, with the Director of DNS.

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 DNS regarding these requirements.

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

Classified Documents From Other Agencies (9) (continued)

**Control of Secret and Confidential Documents Received
Without Required Markings (d)**

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

Destruction of Secret and Confidential Documents (10)

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 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. See MD 12.5, "NRC Automated Information Security Program," for procedures on the destruction of storage media. (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, "Property Management." (iii)

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

Destruction of Secret and Confidential Documents (10)
(continued)

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

Loss or Possible Compromise of Classified Information (11)

DNS and 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)

If the information was originated by another agency, DFS, in consultation with DNS, 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, in conjunction with DNS, 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 E.O. 12958, as amended, Section 2.2, for the classification of NSI. There are also classification guides for RD and FRD.

Classification Guides (D) (continued)

Types of Guides (1)

Within NRC, program classification guides are used for the following purposes:

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

Approval of Guides (2)

The Deputy Executive Director for Reactor and Preparedness Programs (DEDR) 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 of DNS for approval before it is issued. (b)

Review of Guides (3)

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

Classification Guides (D) (continued)

Dissemination of Guides (4)

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

Content of Guides (5)

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)
- Provide the date of issuance or last review (b)
- State precisely the elements of information to be protected, indicate which classification level applies to each element of information, and specify the elements that are unclassified (c)
- State special handling caveats (d)
- Prescribe a specific declassification instruction (i.e., date or event) (e)
- Specify the exemption category identified in E.O. 12958, as amended, Section 3.3(b) (f)
- State a concise reason for classification (g)

Classification Appraisals (E)

Classification appraisals are conducted by DNS 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

Classification Appraisals (E) (continued)

implementation of NRC policy and standards. DNS has appraisal guidance for the standard format used for classification appraisals.

Frequency of Appraisals (1)

The Director of DNS 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, 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)

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 of DNS. (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. DNS 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 E.O. 12829, "National Industrial Security Program." 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 information 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, "Contract Security and/or Classification Requirements" [available on InForms]), the Division of Contracts (ADM) shall forward the NRC Form 187 and Statement of Work to DNS for assessment to determine whether or not a reasonable basis exists for concluding that a compromise or an unauthorized disclosure of classified information may occur. (1)

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)

DNS 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)

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

- Nature and extent of FOCI, including whether a foreign person occupies a controlling or dominant minority position, and the source of FOCI, including 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)

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

- Direct or indirect ownership of 5 percent or more of the 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 nonvoting 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)
- Contracts, agreements, understandings, or arrangements between the applicant company and a 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

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

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, DNS shall review the case to determine the relative significance of the information relative to the factors listed under Sections (F)(3) and (4) above, the extent to which FOCI could result in unauthorized access to classified information, and the type of actions necessary to reduce the effects of FOCI to an acceptable level. However, if DNS determines a company is under FOCI, DNS shall suspend the FCL. (5)

Part II

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.

Access Lists (1)

Access to Top Secret information and NSCI requires a "Q" clearance, a 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 DNS. Additionally, a copy of the NSCI access list for each region and office must be distributed in accordance with Section (C)(2) of this part. (b)

Any updates (e.g., additions or changes) of a regional or office access list must be reported immediately to DNS and any other recipient of the list. (c)

Each region and office will review its access lists during January of each year to ensure that all listed personnel need continued authorization and will provide DNS and any other recipient with a revised list on or before January 31 of each year. (d)

Sanctions (2)

NRC employees, NRC contractors, and other organizations associated with the NRC program shall be subject to appropriate sanctions if they— (a)

Control of Top Secret Documents (A) (continued)

Sanctions (2) (continued)

- Knowingly, willfully, or negligently disclose to unauthorized persons information properly classified under E.O. 12958, as amended, or predecessor Executive Orders, or the AEA. (i)
- Knowingly and willfully classify or continue the classification of information in violation of E.O. 12958, as amended, or any implementing directive. (ii)
- Knowingly and willfully violate any other provision of E.O. 12958, as amended, or any implementing directive, or the AEA relating to the classification and declassification of RD and FRD. (iii)

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. (b)

Central Top Secret Control Officer and Top Secret Control Officers (3)

Central Top Secret Control Officer (a)

The Director of the Division of Nuclear Security (DNS), Office of Nuclear Security and Incident Response, has assigned central control functions for Top Secret information to the Information Security Section (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)

Control of Top Secret Documents (A) (continued)

Central Top Secret Control Officer and Top Secret Control Officers (3) (continued)

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 (EDO), and the Deputy Executive Director for Reactor and Preparedness Programs.) (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)
- 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 of DNS 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)

Control of Top Secret Documents (A) (continued)

Central Top Secret Control Officer and Top Secret Control Officers (3) (continued)

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

Accountability Control Files (4)

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)
- 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 [NSI], Restricted Data [RD], Formerly Restricted Data [FRD]) and control caveats (vi)

Control of Top Secret Documents (A) (continued)

Accountability Control Files (4) (continued)

Receipt File (b)

The receipt file contains records of 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 DNS.

Document History File (c)

The document history file contains a copy of 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 (5)

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.

Physical Inventory (6)

Top Secret documents under the control of the CTSCO, as well as Top Secret documents charged out to authorized recipients, must

Control of Top Secret Documents (A) (continued)

Physical Inventory (6) (continued)

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, the abbreviated title or subject, the copy number and series, the document date, the date of transfer to the authorized holder, and the 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 DNS, 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 126, "Classified Document Receipt," must be used when transmitting a Top Secret document to authorized custodians. (ii)

Control of Top Secret Documents (A) (continued)

Physical Inventory (6) (continued)

- Standard Form 703, "Top Secret Cover Sheet" (available in the NRC Supply Store), 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)

Reproduction of Top Secret Documents (7)

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 of DNS. (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)(5) and (6) 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)

Control of Top Secret Documents (A) (continued)

Reproduction of Top Secret Documents (7) (continued)

"Series _____ Copy _____ of _____ copies."

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

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

Reproduction of Top Secret Documents From Other Agencies (8)

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.

Transmission of Top Secret Documents (9)

Top Secret documents may only be transmitted by approved means. These approved means include the Defense Courier Service, hand carried by specifically authorized NRC and NRC contractor employees, and electronically transmitted through appropriately encrypted telecommunication circuits. Transmission of classified information in the Agencywide Documents Access and Management System (ADAMS) or in the Electronic Information Exchange is prohibited. Procedures applicable to handling classified messages within approved communications centers are set forth in MD 12.4, "NRC Telecommunications Systems Security Program." Under no circumstances may Top

Control of Top Secret Documents (A) (continued)

Transmission of Top Secret Documents (9) (continued)

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 of DNS or by secure communications approved by the Director of DNS. 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, including electronic 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 by commercial airlines must be obtained from the Director of DNS. Additionally, the Transportation Security Administration (TSA) has issued regulations for screening travelers and matter transported by air. (c)

Receipts (10)

NRC Form 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.

Control of Top Secret Documents (A) (continued)

Destruction of Top Secret Documents (11)

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)

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 the CTSCO. (b)

Naval Nuclear Propulsion Information (B)

U.S. naval nuclear propulsion information may be either classified or unclassified information. It must be made available on a need-to-know basis only to appropriately cleared (L clearance for access up to Secret National Security Information [NSI] and Q clearance for access to Secret Restricted Data [SRD] and above) NRC employees and NRC contractor employees who are U.S. citizens. Further explanations of the applicable clearances needed to access U.S. naval nuclear propulsion information can be obtained in MD 12.3, "NRC Personnel Security Program," Part I(B)(2)(b). (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 DNS. DNS is also available to provide assistance. (2)

Public release of classified and unclassified naval nuclear propulsion information, or foreign release thereof, is not permitted. Any request under the Freedom of Information Act (FOIA) from a source outside NRC for nuclear propulsion documents or information must be forwarded through the Office Information

Naval Nuclear Propulsion Information (B) (continued)

Systems (OIS) 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. Storage and dissemination of classified or unclassified naval nuclear propulsion documents in ADAMS is prohibited. (4)

The Office of Naval Reactors, DOE, in providing either classified or unclassified naval nuclear propulsion documents to 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 the following marking: (5)

This document may not be further distributed by any holder without the prior approval of the Office of Naval Reactors, DOE. Distribution to U.S. 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)

National Security Council
Information (C) (continued)

Responsibilities (1) (continued)

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. (a)

The Offices of the Chairman, the Commissioners, and the 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 Section, Office of the EDO. SECY and the Administrative and Correspondence Section will provide a copy of these access lists to the Director of DNS. (c)

National Security Council
Information (C) (continued)

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)

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 Section 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 Section also will forward the NSC cover sheet generated for staff distribution to SECY for storage with the document. (v)

National Security Council
Information (C) (continued)

Requirements (3) (continued)

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 Section, 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)

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 _____" on and assign a sequential alphabetical designator (i.e., A, B, C, etc.) to each copy of the document. (ii)

National Security Council
Information (C) (continued)

Requirements (3) (continued)

Documents Generated by NRC (c)

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 worksheets must be protected. Additionally, the office generating the NSCI document must contact SECY to obtain guidance for accountability of the document.

Loss or Possible Compromise of Documents (d)

DNS 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. DNS 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. Any resulting corrective action resulting from the infraction must be communicated to OIG.

Classification, Declassification, or Downgrading (e)

Any classification, declassification, or downgrading questions on NSCI must be referred to DNS for advice and assistance.

Requests for Information Under the Freedom of Information Act (f)

SECY, in consultation with the Office of the General Counsel (OGC), will determine what NSCI records, if any, are subject to the FOIA. OIS must be notified when NSCI records are the subject

Transfer of Classified Information to Foreign Governments and International Organizations (D)

of a FOIA request. OIS will be responsible for referring the records to the NSC.

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 RD or FRD to foreign governments or international organizations. RD and FRD 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, as amended (ERA), or by any international agreement to which the United States is a party, or by U.S. 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 by the Director of the Office of International Programs (OIP). 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 ERA, 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)

Transfer of Classified Information to
Foreign Governments and
International Organizations (D) (continued)

Criteria (2) (continued)

- Consistent with the national security interests of the United States (*c*)
- Limited to information necessary to the purpose for which disclosures are made (*d*)
- 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

Transfer of Classified Information to
Foreign Governments and
International Organizations (D) (continued)

Criteria (2) (continued)

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 the 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 criteria of Section (D)(2)(a) of this part have been waived by the Commission. (ii)

Responsibilities (3)

The Director of 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 determination must be made with the concurrence of OGC, DNS/NSIR, 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, DNS will determine whether an applicable prerequisite government-to-government agreement exists between the United States and the foreign country involved. (i)

Transfer of Classified Information to
Foreign Governments and
International Organizations (D) (continued)

Responsibilities (3) (continued)

If an agreement exists, DNS, 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)(ii) of this part concerning the criteria specified. The Commission will also approve any waiver of the requirement for a separate classified exchange agreement referenced in Section (D)(3)(a)(ii) of this part. (iv)

Agreements with foreign governments will not commit NRC to disclose any particular or specific classified information. (v)

**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

Transfer of Classified Information to
Foreign Governments and
International Organizations (D) (continued)

Responsibilities (3) (continued)

reason for providing classified information. Therefore, before permitting representatives of international organizations (with the exception of the IAEA) access to classified information, DNS must be consulted. (i)

DNS will coordinate the matter with OIP, OGC, and others, as appropriate, and approve or disapprove the access. If the access is approved, DNS 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)

Security assurances will be obtained from an authorized person of a foreign government. Upon receipt, the names of the representatives of foreign governments who need access to classified information will be submitted by DNS for appropriate security checks. (b)

The EDO is authorized by PDD 1958 on Foreign Disclosure and SECY-78-84, "Transfer of Classified Non-military Information to Foreign Governments by NRC," 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)

Transfer of Classified Information to
Foreign Governments and
International Organizations (D) (continued)

Internal Procedures (4) (continued)

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 DNS. DNS shall make available any derogatory information derived from security checks on a confidential basis to only the Director of OIP and the EDO.

Review of Information To Be Shared With Foreign Governments (iii)

Classified documents to be transmitted to foreign governments must be forwarded to DNS 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. (1)
- 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. (2)
- Concurrence in the legal aspects of the transfer has been obtained from OGC. (3)

Transfer of Classified Information to
Foreign Governments and
International Organizations (D) (continued)

Internal Procedures (4) (continued)

If the transfer involves classified documents or other classified information originated, produced, or received from another department or agency, DNS will obtain approval from this department or agency. (c)

Classified information to be shared with foreign governments within NRC must be coordinated with DNS in advance to ensure the procedures in Section (D)(4)(a)(iv) of this part are observed. (d)

Accountability (iv)

A record of accountability of the information being processed for release must be maintained by DNS 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) (1)
- Names and signatures of approving officials (2)
- Form in which information is released or will be released (e.g., oral or documentary) (3)
- Date of release or contemplated release (4)

Transfer of Classified Information to
Foreign Governments and
International Organizations (D) (continued)

Internal Procedures (4) (continued)

- Identity of foreign government organization and the original individual recipient to whom release is made or is contemplated (5)
- Security assurance and security check, when applicable, for each individual recipient (6)
- Waivers exercised or requested, when applicable (7)
- Statement that the information is based on data originated outside NRC, wherever applicable, and the identity of the originating organization (8)
- Name of individual in other U.S. Government agency who has authorized release, if applicable (9)

The office or division contemplating or making oral disclosures must furnish memoranda before and after these disclosures to the Directors of DNS 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. Classified information to be transmitted to foreign governments will use government-to-government mail channels. 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 of DNS.

Transfer of Classified Information to
Foreign Governments and
International Organizations (D) (continued)

Internal Procedures (4) (continued)

**Transfer of Classified Information to International
Organizations (Except IAEA) (b)**

The transfer of classified information to international organizations, except IAEA (see Section (D)(4)(c) of this part), must be handled in accordance with guidance from DNS.

Transfer of Classified Information to IAEA (c)

Written Disclosure Authorization (i)

A written disclosure authorization from DNS is required before IAEA representatives may have access to NSI. 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 (1)
- Specific authority to disclose NSI to that individual relating to the visit or inspection (2)
- The level of classified information authorized (3)
- A description of the IAEA representative's identification documents (4)
- The purpose of the visit or inspection (5)

Transfer of Classified Information to
Foreign Governments and
International Organizations (D) (continued)

Internal Procedures (4) (continued)

- The duration of the authorization to receive the information (6)

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 DNS 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, DNS will obtain approval from the department or agency before access or transmission. (b)

Accountability (iii)

See Section (D)(4)(a)(iv) of this part.

Preparation and Method of Transmission (iv)

See Section (D)(4)(a)(v) of this part.

Report to the National Disclosure Policy Committee (NDPC) (v)

DNS 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

Transfer of Classified Information to
Foreign Governments and
International Organizations (D) (continued)

Internal Procedures (4) (continued)

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.

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 Section I (B)(2) of this handbook) or to DNS for review before unclassified use. (a)
- 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 DNS before presentation. (b)

Classified Conferences (E) (continued)

Publication or Release of Documents (2)

When there is doubt as to whether a document contains NSI, RD, or FRD, the author shall refer the information to the appropriate NRC authorized classifier or the Director of DNS 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 DNS for review. If, after review, it is determined that the article contains information that should be classified, DNS will advise the author, to the extent possible within the bounds of security and the NRC's "No Comment" Policy, 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, DNS 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, "NRC Personnel Security Program," or by persons formerly or currently cleared by other Government agencies must be reviewed by an NRC authorized classifier or by DNS. The author shall be required to delete any classified information in the document before it is published.

Hand-carrying Classified Material (F)

An authorized person hand-carrying classified information from an NRC facility, licensee, or other Government agency for return to NRC, regardless of the duration or distance of the trip, must obtain authorization from the Director of DNS.

Courier Letters (1)

A letter of Courier Authorization from the Director of DNS is required when hand-carrying classified information is deemed necessary. The authorized person must also sign a courier procedures agreement in the presence of the issuing official. A new authorization letter is required for each period of courier activity.

Courier Card (2)

A courier card from the Director of DNS is issued in lieu of a courier letter for those authorized persons who require the handling and transporting of classified material on a regular basis. When no longer needed, the card will be returned to the issuing office, which will hold the card until it is needed or it expires.

Transporting Classified Material by Commercial Airlines (G)

Approval for NRC employees or contractor employees to hand-carry classified documents during travel by commercial airlines must be obtained from the Director of DNS. Additionally, the Transportation Security Administration (TSA) 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 on it. 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 TSA security representative and explain the situation. If necessary, the traveler will contact his or her own supervisor or DNS. (c)
- When the classified documents to be transported are of a size, weight, or shape not suitable for the processing specified above, the following procedures apply: (d)

Transporting Classified Material by Commercial Airlines (G) (continued)

- 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 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)

Transporting Classified Material by Commercial Airlines (G) (continued)

- 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)
- 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 stationery of the agency or the contractor being visited. (3)

Exhibit 4 Upgrading, Downgrading, and Transclassification Markings

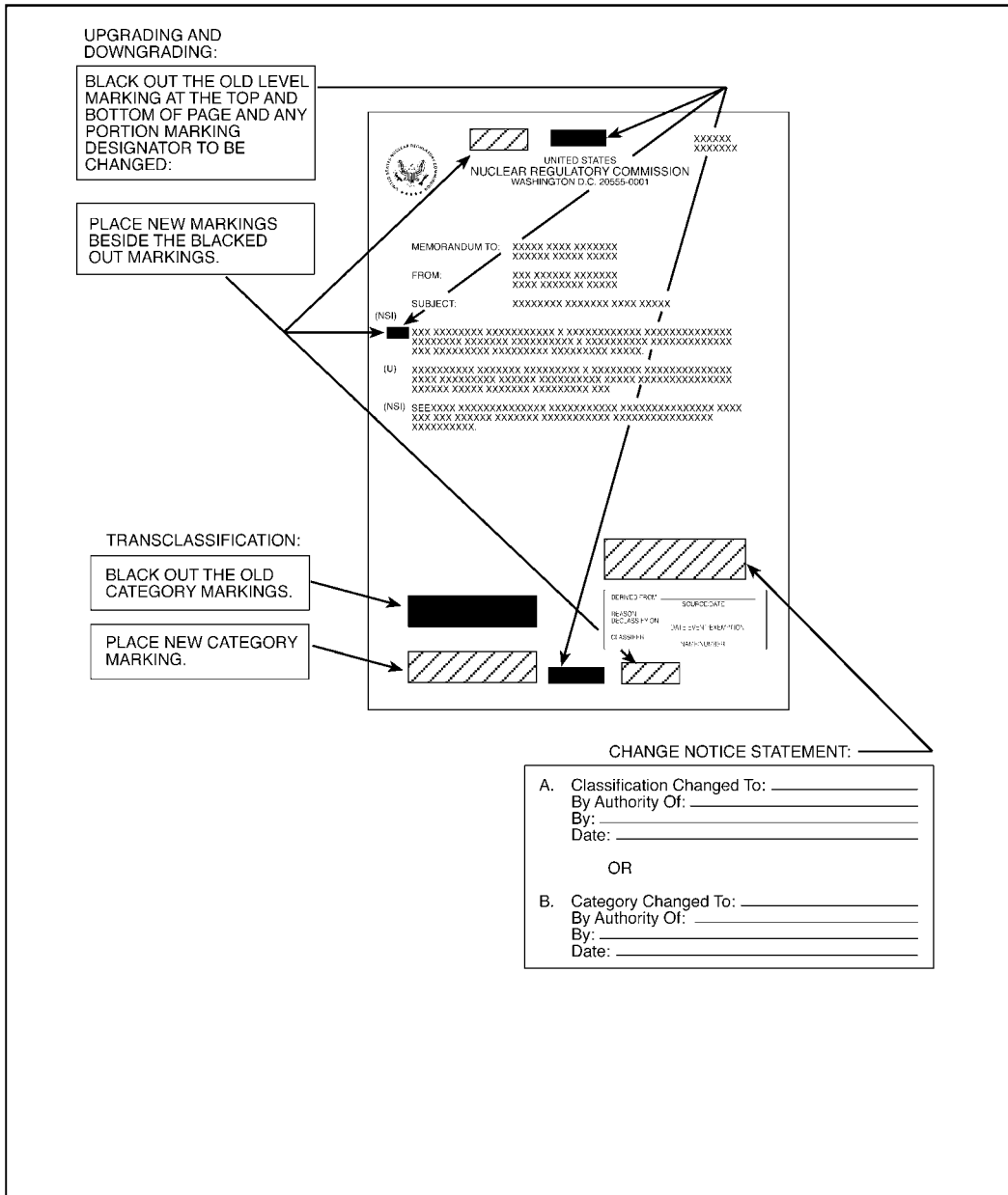


Exhibit 5 Deleting Classified Information From Classified Documents

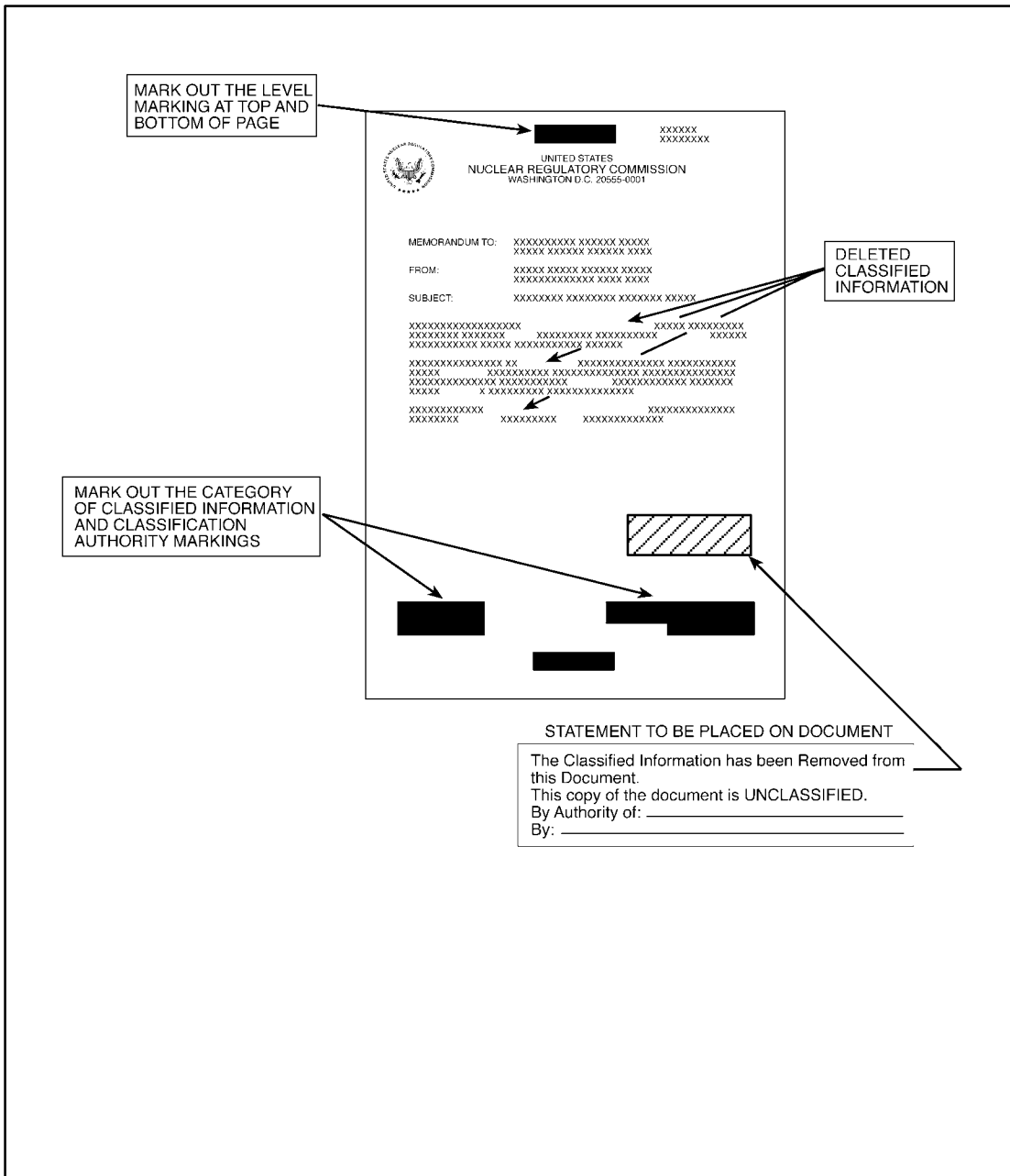


Exhibit 7 Required Markings for a Classified Transmittal Document

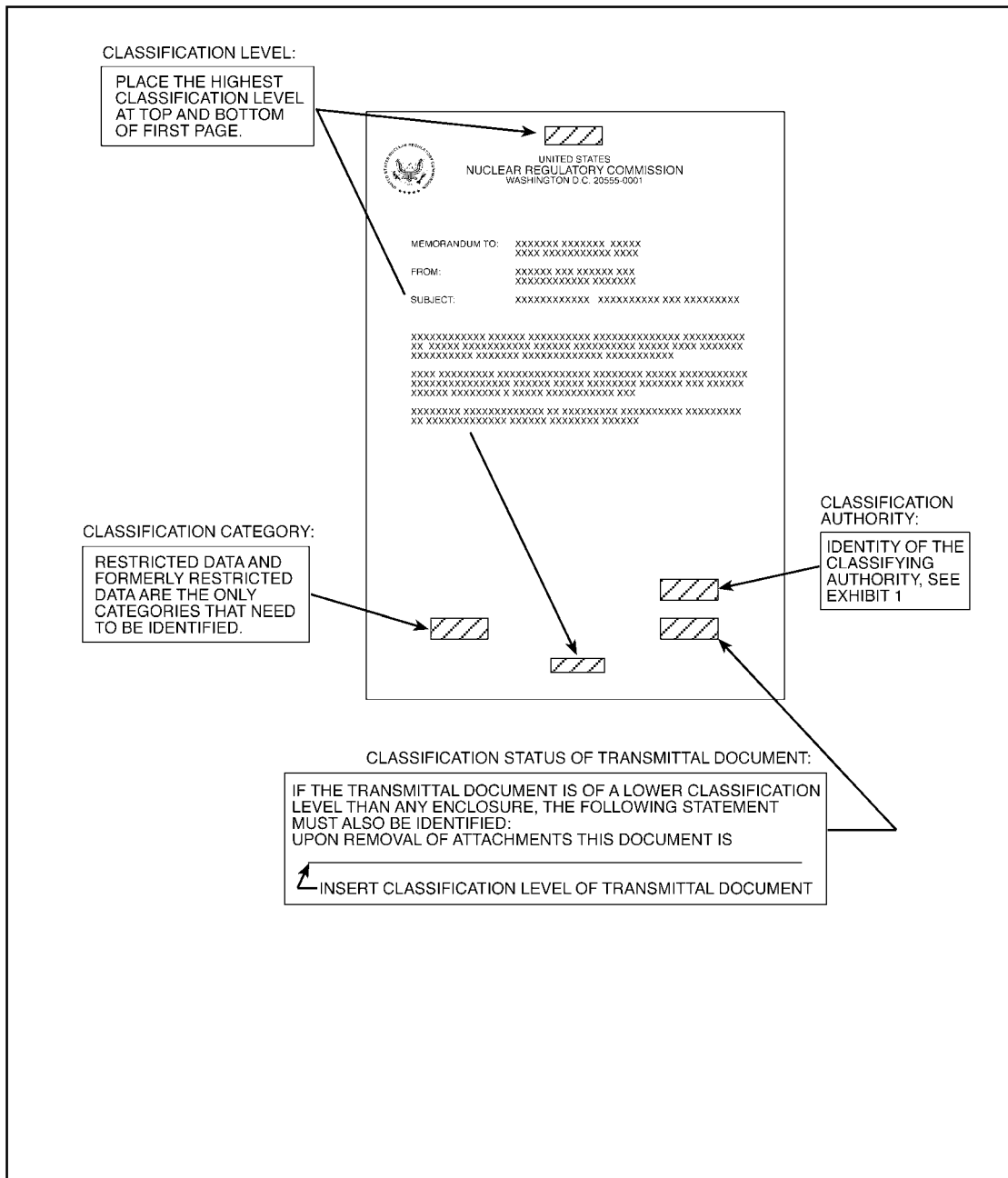


Exhibit 8 Required Markings for Envelopes or Wrappers

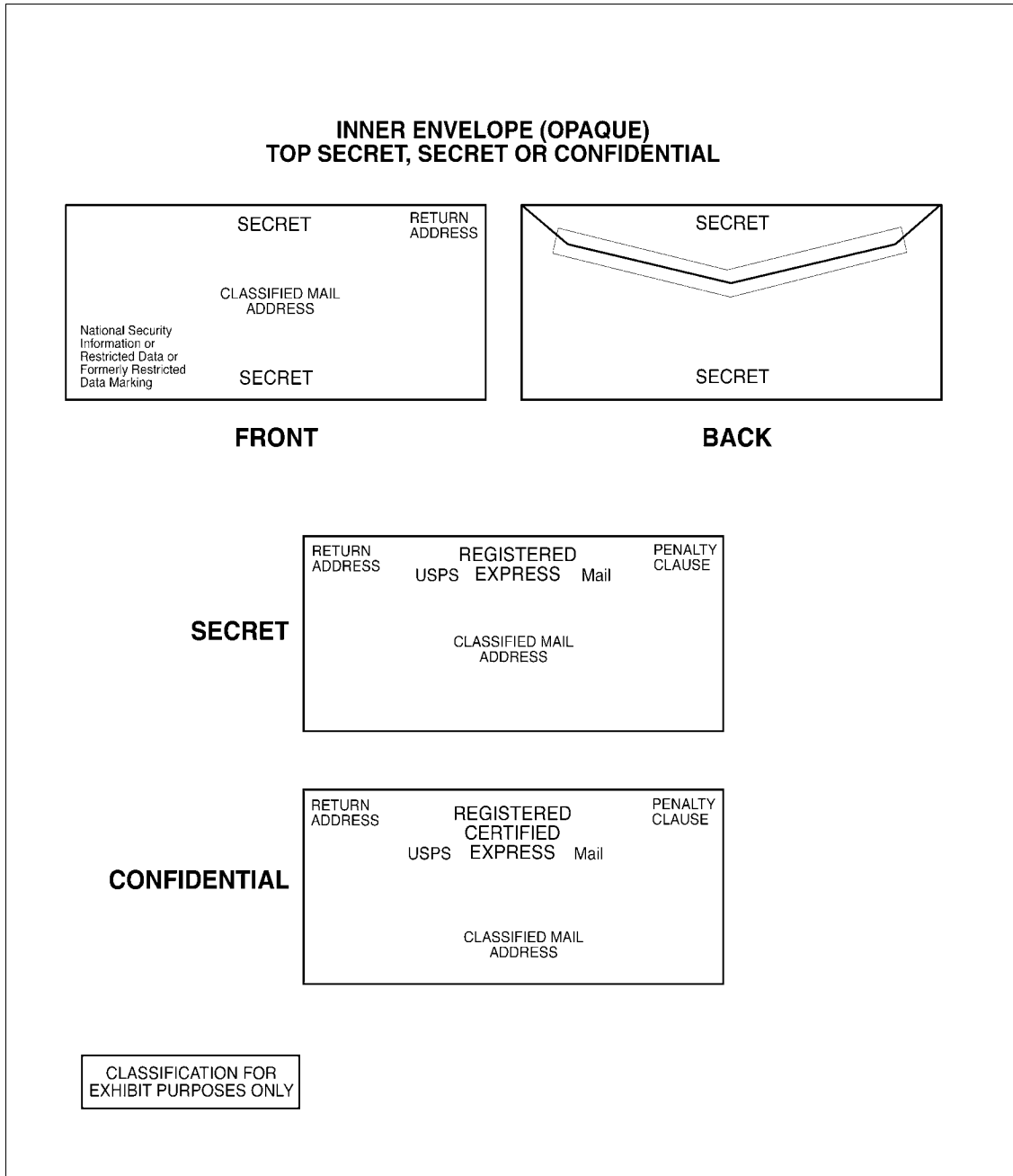


Exhibit 9 Foreign Equivalent Markings

Country	Top Secret	Secret	Confidential	Restricted
Argentina	Estrictamente Secreto	Secreto	Confidencial	Reservado
Australia	Top Secret	Secret	Confidential	Restricted
Austria	Streng Geheim	Geheim	Verschluss	
Belgium (Flemish)	Zeer Geheim	Geheim	Vertrouwelijk	Bepertke Verspreiding
Bolivia	Supersecreto or Muy Secreto	Secreto	Confidencial	Reservado
Brazil	Ultra Secreto	Secreto	Confidencial	Reservado
Cambodia	Sam Ngat Bamphot	Sam Ngat	Roeung Art Kambang	Ham Kom Psay
Canada	Top Secret	Secret	Confidential	Restricted
Chile	Secreto	Secreto	Reservado	Reservado
Columbia	Ultrasecreto	Secreto	Reservado	Confidencial Restringido
Costa Rica	Alto Secreto	Secreto	Confidencial	
Denmark	Yderst Hemmeligt	Hemmeligt	Fortroligt	Tiltjenestebrug
Ecuador	Secretisimo	Secreto	Confidencial	Reservado
El Salvador	Ultra Secreto	Secreto	Confidencial	Reservado
Ethiopia	Yemiaz Birtou Mistir	Mistir	Kilkil	
Finland	Erittain Salainen	Salainen		

Exhibit 9 (continued)

Country	Top Secret	Secret	Confidential	Restricted
France	Tres Secret	Secret Defense	Confidentiel Defense	Diffusion Restreinte
Germany	Streng Geheim	Geheim	Vs-Vertraulich	
Greece	ΑΚΡΩΣ ΑΠΟΡΡΗΤΟΝ	ΑΠΟΡΡΗΤΟΝ	ΕΜΠΙΣΤΕΥΤΙΚΟΝ	ΠΕΡΙΩΡΙΣΜΕΝΗΣ ΧΡΗΣΕΩΣ
Guatemala	Alto Secreto	Secreto	Confidencial	Reservado
Haiti	Top Secret	Secret	Confidential	Reserve
Honduras	Super Secreto	Secreto	Confidencial	Reservado
Hong Kong	Top Secret	Secret	Confidential	Restricted
Hungary	Szigoruan Titkos	Titkos	Bizalmas	
India	Param Gupt	Gupt	Gopniya	Pratibandhs/seemita
Indonesia	Sangat Rahasia	Rahasia	Agak Rahasia	Terbatas
Iran	Bekoliserri	Serri	Kheil Mahramaneh	Mahramaneh
Iraq	Sirri Lil-ghaxah	Sirri	Khass	Mehdoud
Ireland	Algjorti	Trunadarmal		
Ireland (Gaelic)	An-sicreideach	Sicreideach	Runda	Srianta
Israel	Sodi Beyoter	Sodi	Shamur	Mugbal
Italy	Segretissimo	Segreto	Riservatissimo	Riservato
Japan	Kimitsu	Gokuhi	Hi	Toriatsukaichui
Jordan	Maktum Jiddan	Maktum	Sirri	Mahdud
Korea	I-Kup Bi Mil	II-Kup Bi Mil	III-Kup Bi Mil	Bu Woi Bi

Exhibit 9 (continued)

Country	Top Secret	Secret	Confidential	Restricted
Laos	Lup Sood Gnod	Kuam Lup	Kuam Lap	Chum Kut Kon Arn
Lebanon	Tres Secret	Secret	Confidentiel	
Mexico	Alto Secreto	Secreto	Confidencial	Restringido
Netherlands	Zeer Geheim	Geheim	Confidentieel or Vertrouwelijk	Dienstgeheim
New Zealand	Top Secret	Secret	Confidential	Restricted
Nicaragua	Alto Secreto	Secreto	Confidencial	Reservado
Norway	Strengt Hemmelig	Hemmelig	Konfidensiell	Begrenset
Pakistan (URDU)	Intahai Khufia	Khufia	Sigha-E-Raz	Barai Mahdud Taqsim
Paraguay	Secreto	Secreto	Confidencial	Reservado
Peru	Estrictamente Secreto	Secreto	Confidencial	Reservado
Philippines	Top Secret	Secret	Confidential	Restricted
Portugal	Muito Secreto	Secreto	Confidencial	Reservado
Saudi Arabia	Saudi Top Secret	Saudi Very Secret	Saudi Secret	Saudi Restricted
Spain	Maximo Secreto	Secreto	Confidencial	Diffusion Limitada
Sweden (red borders)	Hemlig	Hemlig		
Switzerland	(Three languages: French, German and Italian. TOP SECRET has a registration number to distinguish from SECRET and CONFIDENTIAL)			
Taiwan	Chichimi	Chimi		
Thailand	Lup Tisud	Lup Maag	Lup	Pok Pid
Turkey	Cok Gizli	Gizli	Ozel	Hizmete Ozel

Exhibit 9 (continued)

Country	Top Secret	Secret	Confidential	Restricted
Union of South Africa	Top Secret	Secret	Confidential	Restricted
English				
Afrikaans	Uiters Geheim	Geheim	Vertroulik	Beperk
United Arab Republic of Egypt	Jirri Lilghaxeh	Sirri	Khas	Mehoud Jidden
United Kingdom	Top Secret	Secret	Confidential	Restricted
Uruguay	Ultra Secreto	Secreto	Confidencial	Reservado
Russia	СОВЕРШЕННО СЕКРЕТНО	СЕКРЕТНО	НЕ ПОДЛЕЖАЩИЙ ОГЛАШЕНИЮ	ДЛЯ СЛУЖЕБНОГО ПОЛЬЗОВАНИЯ
Viet Nam (Vietnamese)	Toi-Mat	Mat	Kin	Pho Bien Han Che