U.S. NUCLEAR REGULATORY COMMISSION

DIRECTIVE TRANSMITTAL

TN: DT–99–11

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

NRC Classified Information Security Program

Directive 12.2

Contents

Policy 1

Objective 1

Organizational Responsibilities and Delegations of Authority 1

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

Applicability 5

Handbook 5

Exceptions or Deviations 5

References 5

NRC Classified Information Security Program
Directive 12.2

Policy
(12.2–01)

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

Objective
(12.2–02)

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

Organizational Responsibilities and Delegations of Authority
(12.2–03)

Chairman
(031)

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

Approved: May 13, 1993
(Revised: April 27, 1999)

The Commission
(032)

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

Secretary of the Commission
(033)

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

Executive Director for Operations (EDO)
(034)

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

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

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

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

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

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

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

Director, Office of Administration (ADM)
(037)

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

Office Directors and Regional Administrators
(038)

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

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

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

Applicability
(12.2–04)

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

Handbook
(12.2–05)

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

Exceptions or Deviations
(12.2–06)

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

References
(12.2–07)

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

Code of Federal Regulations—

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

10 CFR Part 9, "Public Records."

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

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

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

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

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

References
(12.2–07) (continued)

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

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

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

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

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

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

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

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

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

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

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

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

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

NRC Management Directive—

3.1, "Freedom of Information Act."

3.2, "Privacy Act."

5.5, "Public Affairs Program."

12.1, "NRC Facility Security Program."

12.3, "NRC Personnel Security Program."

References
(12.2–07) (continued)

12.4, "NRC Telecommunications Systems Security Program."

12.5, "NRC Automated Information Systems Security Program."

12.6, "NRC Sensitive Unclassified Information Security Program."

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

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

NRC Classified Information Security Program

Handbook 12.2

Contents

Part I

Protection and Control of Classified Information 1

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

Contents (continued)

Part II

Protection and Control of Foreign Intelligence Information 41

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

Part III

Special Handling of Classified Information 50

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

Contents (continued)

Part III (continued)

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

Exhibits

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

Contents (continued)

Exhibits (continued)

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

Part I

Protection and Control of Classified Information

Scope (A)

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

Classification (B)

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

Responsibilities To Protect Classified Information (1)

Classification Determinations (a)

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

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

Classification (B) (continued)

Responsibilities To Protect Classified Information (1) (continued)

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

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

Delegation of Classification Authority (b)

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

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

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

Classification (B) (continued)

Responsibilities To Protect Classified Information (1) (continued)

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

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

Authorized Classifier Training (c)

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

Responsibilities of Authorized Classifiers (d)

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

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

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

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

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

Classification (B) (continued)

Responsibilities To Protect Classified Information (1) (continued)

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

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

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

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

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

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

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

Classification (B) (continued)

Responsibilities To Protect Classified Information (1) (continued)

Responsibilities of Originators (d)

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

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

Classification Challenges (e)

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

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

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

Classification (B) (continued)

Responsibilities To Protect Classified Information (1) (continued)

Limitations on Classification (f)

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

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

Classification of Protected Information (2)

Classification Process (a)

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

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

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

National Security Information (i)

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

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

Classification (B) (continued)

Classification of Protected Information (2) (continued)

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

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

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

Restricted Data and Formerly Restricted Data (ii)

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

Classification (B) (continued)

Classification of Protected Information (2) (continued)

Levels of Classification (c)

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

Sensitivity of the Information (i)

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

Classification Authority (ii)

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

Duration of Classification (iii)

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

Declassification Exemptions (iv)

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

Classification (B) (continued)

Classification of Protected Information (2) (continued)

Classification Extensions (v)

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

Information Classified Under Previous Executive Orders (vi)

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

Restricted Data and Formerly Restricted Data Exemption (vii)

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

Marking Classified Documents (3)

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

Classification (B) (continued)

Marking Classified Documents (3) (continued)

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

Category of Classified Information (a)

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

Classification Markings for National Security Information (b)

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

Classified By: David Smith, Chief, ABC Branch

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

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

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

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

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

Classification (B) (continued)

Marking Classified Documents (3) (continued)

Classification Markings for Restricted Data (c)

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

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

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

Classified By: Classification Guide ABC

Derivative Classifier: _____
(Name and Title)

Declassification Markings (d)

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

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

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

Classification Authority (e)

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

Classification (B) (continued)

Marking Classified Documents (3) (continued)

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

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

Portion Marking (f)

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

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

  (TS) for Top Secret

  (S) for Secret

  (C) for Confidential

  (U) for Unclassified

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

  (RD) for Restricted Data

  (FRD) for Formerly Restricted Data

Classification (B) (continued)

Marking Classified Documents (3) (continued)

(NSI) for National Security Information

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

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

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

Change of Classification and Marking (4)

Upgrading (a)

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

Classification (B) (continued)

Change of Classification and Marking (4) (continued)

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

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

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

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

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

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

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

Classification (B) (continued)

Change of Classification and Marking (4) (continued)

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

Classification changed to: (insert new level)

By authority of: (person authorizing change)

By: (signature of person making change)

Date: (date of change)

Downgrading (b)

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

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

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

Classification (B) (continued)

Change of Classification and Marking (4) (continued)

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

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

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

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

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

Classification (B) (continued)

Change of Classification and Marking (4) (continued)

Classification changed to: (insert new level)

By authority of: (person authorizing change)

By: (signature of person making change)

Date: (date of change)

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

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

Transclassification (c)

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

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

Classification (B) (continued)

Change of Classification and Marking (4) (continued)

Category changed to: (insert new category)

By authority of: (person authorizing change)

By: (signature of person making change)

Date: (Date of change)

Declassification of National Security Information (5)

Authorities (a)

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

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

Automatic Declassification (b)

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

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

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

Classification (B) (continued)

Declassification of National Security Information (5) (continued)

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

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

Declassification Reviews (c)

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

Standard Declassification Reviews (i)

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

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

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

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

Classification (B) (continued)

Declassification of National Security Information (5) (continued)

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

Mandatory Review for Declassification (iii)

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

Systematic Review for Declassification (iv)

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

Notice of Declassification (v)

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

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

Classification (B) (continued)

Declassification of National Security Information (5) (continued)

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

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

Deletion of Classified Information From Documents (6)

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

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

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

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

Classification (B) (continued)

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

The classified information has been removed from this document.

This copy of the document is UNCLASSIFIED.

By Authority of: (person authorizing deletion)

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

Markings for Specific Types of Classified Information (7)

Transmittal Documents (a)

Unclassified Transmittal Documents (i)

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

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

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

Classified Transmittal Documents (ii)

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

Classification (B) (continued)

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

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

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

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

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

Compilations (iii)

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

Files or Folders Containing Classified Documents (iv)

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

Classification (B) (continued)

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

Drafts and Working Copies (b)

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

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

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

Reproduction and Dissemination Limitations (c)

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

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

Foreign Government Information (d)

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

Classification (B) (continued)

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

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

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

Word Processor Disks (e)

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

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

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

Classification (B) (continued)

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

Translations (f)

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

Record Classification Actions (RCA) System (8)

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

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

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

Control of Secret and Confidential Documents (C)

Cover Sheets (1)

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

Assurances Required Before Transmission of Classified Information (2)

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

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

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

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

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

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

Means of Transmission of Secret Documents (3)

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

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

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

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

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

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

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

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

Means of Transmission of Confidential Documents (4)

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

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

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

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

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

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

Electronically Transmitted Classified Messages (5)

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

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

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

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

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

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

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

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

Electronically Transmitted Classified Messages (5) (continued)

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

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

Transmission of Documents From Other Agencies (6)

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

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

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

Preparation of Secret and Confidential Documents for Transmission (7)

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

Preparation of Receipts (a)

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

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

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

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

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

Verification, Signature, and Return of Receipts (b)

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

Envelopes and Wrappers (c)

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

Inner Envelope or Wrapper (i)

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

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

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

Outer Envelope or Wrapper (ii)

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

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

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

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

Evidence of Tampering (iii)

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

Classified Documents From Other Agencies (8)

Safeguards To Be Afforded (a)

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

Third Agency Rule (b)

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

Registered Documents (c)

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

Responsibility for Change of Classification and Declassification (d)

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

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

Classified Documents From Other Agencies (8) (continued)

Documents Received Without Required Markings (e)

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

Destruction of Secret and Confidential Documents (9)

Responsibilities (a)

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

Method of Destruction (b)

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

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

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

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

Loss or Possible Compromise of Classified Information (10)

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

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

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

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

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

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

Classification Guides (D)

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

Types of Guides (1)

Within NRC, classification guides are grouped in the following types

Program Classification Guides (a)

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

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

Local Classification Guides (b)

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

Classification Guides (D) (continued)

Contents of Guides (2)

Classification guides must—

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

Approval of Guides (3)

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

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

Review of Guides (4)

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

Dissemination of Guides (5)

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

Content of Guides (6)

As a minimum, classification guides should—

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

Classification Guides (D) (continued)

Content of Guides (6) (continued)

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

Classification Appraisals (E)

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

Frequency of Appraisals (1)

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

Reports (2)

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

Classification Appraisals (E) (continued)

Reports (2) (continued)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Part II

Protection and Control of Foreign Intelligence Information

Scope (A)

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

Access to Foreign Intelligence Information (B)

Authorization for Access (1)

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

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

Access to Foreign Intelligence Information (B) (continued)

Authorization for Access (1) (continued)

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

Emergency Authorization for FII Access (2)

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

Security Education and Awareness Briefing (3)

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

Termination of Access (4)

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

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

Access to Foreign Intelligence Information (B) (continued)

Contractors and Consultants (5)

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

Control of Documents (C)

Markings (1)

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

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

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

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

Control of Documents (C) (continued)

Markings (1) (continued)

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

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

Reproduction (2)

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

Control of Documents (C) (continued)

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

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

Release to Other Government Agencies (4)

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

Transmission (5)

To and From Other Government Agencies (a)

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

Within the NRC (b)

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

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

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

Control of Documents (C) (continued)

Transmission (5) (continued)

Between Installations (c)

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

Abroad (d)

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

Required Envelopes or Wrappers (e)

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

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

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

Cover Sheets (f)

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

Control of Documents (C) (continued)

Transmission (5) (continued)

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

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

Accountability (6)

Centralized Control (a)

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

Access Sheets (b)

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

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

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

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

Control of Documents (C) (continued)

Classified Meetings or Presentations (7)

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

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

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

Storage (8)

Type of Security Containers (a)

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

Access to Containers (b)

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

Changes to Security Container Combinations (c)

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

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

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

Control of Documents (C) (continued)

Destruction (9)

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

Unauthorized Disclosure of Classified FII (D)

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

Classification, Declassification, or Downgrading (E)

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

Part III

Special Handling of Classified Information

Control of Top Secret Documents (A)

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

Top Secret Control Officers (1)

Central Top Secret Control Officer (a)

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

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

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

Control of Top Secret Documents (A) (continued)

Top Secret Control Officers (1) (continued)

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

Top Secret Control Officers (b)

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

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

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

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

Accountability Control Files (2)

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

Document Register (a)

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

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

Control of Top Secret Documents (A) (continued)

Accountability Control Files (2) (continued)

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

Receipts File (b)

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

Document History File (c)

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

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

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

Control of Top Secret Documents (A) (continued)

Physical Inventory (4)

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

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

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

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

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

Control of Top Secret Documents (A) (continued)

Reproduction of Top Secret Documents (5)

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

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

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

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

"Series _____Copy_____ of_____copies."

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

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

Reproduction of Top Secret Documents From Other Agencies (6)

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

Control of Top Secret Documents (A) (continued)

Transmission of Top Secret Documents (7)

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

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

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

Receipts (8)

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

Destruction of Top Secret Documents (9)

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

Control of Top Secret Documents (A) (continued)

Destruction of Top Secret Documents (9) (continued)

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

Naval Nuclear Propulsion Information (B)

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

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

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

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

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

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

National Security Council Information (NSCI) (C)

Responsibilities (1)

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

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

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

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

Access Lists (2)

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

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

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

Requirements (3)

Receipt and Handling (a)

All classified NSCI transmitted to NRC by the National Security Council (NSC) will be addressed to the Chairman and, therefore, received by SECY. (i)

National Security Council Information (NSCI) (C) (continued)

Requirements (3) (continued)

SECY will maintain strict control and accountability over all classified documents containing NSCI. (ii)

Upon receipt of NSCI, SECY will—(iii)

- Record the NSC number affixed to the NSC cover sheet. (*a*)
- Determine who at the Commission level requires access to the information and record the names of the offices on the NSC cover sheet. (*b*)
- Forward the NSCI document to the responsible individual designated on the intended recipient's access list. (*c*)
- Ensure that the document and the NSC cover sheet are returned to SECY for storage after completion of the required circulation and review. (*d*)

If the NSCI document is to be distributed at the staff level, the EDO Administrative and Correspondence Branch will duplicate steps (a) through (d) of item (iii) above for appropriate distribution. (iv)

Upon return of the document from the staff, the EDO Administrative and Correspondence Branch also will forward the NSC cover sheet generated for staff distribution to SECY for storage with the document. (v)

In the event an office receives classified NSCI by means other than those described above, that office will immediately notify SECY. SECY will obtain the NSCI document from the office and follow the procedures under item (iii) above to ensure proper control and accountability. SECY also will notify DFS staff, who will conduct an inquiry into the matter and take the necessary action to prevent recurrence. (vi)

All authorized individuals having access to a classified document containing NSCI shall sign the NSC cover sheet accompanying the document. If an authorized individual is only responsible for distribution of the document (e.g., SECY, EDO Administrative and Correspondence Branch, a designated individual of an office), this individual shall indicate this fact by placing the symbol "DO" (for "distribution only") after his or her signature on the cover sheet. (vii)

National Security Council Information (NSCI) (C) (continued)

Requirements (3) (continued)

Reproduction (b)

Documents containing NSCI will be reproduced only when it is determined that the document must be circulated quickly to facilitate a timely NRC response. The determination that a classified document containing NSCI needs to be reproduced will be made by SECY. Only SECY may reproduce classified NSCI documents. (i)

After making the required copies, SECY will complete and affix an NSC cover sheet to each copy of the document. Above the NSC number on the cover sheet, SECY will place "NRC Copy _____" and assign a sequential alphabetical designator (i.e., A, B, C, etc.) to each copy of the document. (ii)

Documents Generated by NRC (c)

The NRC does not routinely generate documents that contain classified NSCI. However, in the event an office does generate a document that contains classified NSCI, the document and any drafts and work sheets must be protected. Additionally, the office generating the NSCI document must contact DFS to obtain guidance for accountability of the document.

Loss or Possible Compromise of Documents (d)

DFS must be notified immediately in the event of loss or possible compromise of a classified NSCI document. Staff offices shall submit a written report on any such matter to the Chairman through the EDO. Commission offices shall submit a written report on any such matter to the Chairman. DFS will report a loss or a possible compromise to NSC and conduct an inquiry into the matter. A written report on the matter, including corrective measures taken, where appropriate, shall be submitted by the EDO to the Chairman.

Classification, Declassification, or Downgrading (e)

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

National Security Council Information (NSCI) (C) (continued)

Requirements (3) (continued)

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

SECY, in consultation with the Office of the General Counsel, will determine what NSCI records, if any, are subject to the Freedom of Information Act (FOIA). The OCIO must be notified when NSCI records are the subject of FOIA request. OCIO will be responsible for referring the records to the NSC.

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

Authorities (1)

Classified Nonmilitary Information (a)

The Presidential Directive of September 23, 1958, "Basic Policy Governing the Release of Classified Defense Information to Foreign Governments," specifies policy governing the transfer of classified nonmilitary information to foreign governments and access to classified nonmilitary information by individual representatives of foreign governments.

Classified Military Information (b)

Basic policy governing the release and disclosure of classified military information is specified in "National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations," and supplemented by National Security Decision Memorandum (NSDM)-119, "Disclosure of Classified Military Information to Foreign Governments and International Organizations.

Restricted Data and Formerly Restricted Data (c)

The provisions of Section (D) of this part do not apply to the transmission of Restricted Data or Formerly Restricted Data to foreign governments or international organizations. Restricted Data and Formerly Restricted Data are furnished to and received from foreign governments and international organizations only in accordance with Agreements for Cooperation negotiated in accordance with the provisions of Sections 123 and 144 of the Atomic Energy Act of 1954, as amended (AEA).

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

Authorities (1) (continued)

Prohibitions on Disclosure (d)

The disclosure of classified information to foreign governments or international organizations is not permitted when such disclosure is prohibited by Presidential orders or directives, Federal legislation, including the AEA, and the Energy Reorganization Act of 1974 (ERA), as amended, or by any international agreement to which the United States is a party, or by United States policy.

Criteria (2)

Criteria for Release of Classified Information to Foreign Governments (a)

The following criteria must be satisfied before the release of classified nonmilitary information to foreign governments.

- A determination that the furnishing of classified information will result in a net advantage to the national security interests of the United States must be made. In making this determination, disclosure is—(i)
  - Consistent with the foreign policy of the United States toward the recipient government (*a*)
  - Consistent with the policies of the U.S. Government with regard to the AEA, the AEA, or with regard to information for which special procedures for release have been or may hereafter be established by competent authority having statutory jurisdiction over the subject matter (*b*)
  - Consistent with the national security interests of the United States (*c*)
  - Limited to information necessary to the purpose for which disclosures made (*d*)

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

Criteria (2) (continued)

- The recipient government must have agreed, either generally or in the particular case, to—(ii)
  - Not release the information to a third party without the approval of the releasing party (*a*)
  - Afford the information substantially the same degree of protection afforded it by the releasing party (*b*)
  - Not use the information for other than the purpose for which it was given (*c*)
  - Respect rights such as patents, copyrights, or trade secrets, in the event that the releasing party indicates private rights are involved in the information. (*d*)

Criteria for Release of Classified Information to International Organizations (b)

The release of classified information to international organizations, with the exception of the International Atomic Energy Agency (IAEA) noted in the next paragraph, must be on the basis of criteria identified in Section (D)(2)(a) of this part. However, these criteria will be addressed on a case-by-case basis for each transmittal, taking into account the particular reason for providing classified information to that organization. (i)

The Commission has determined that the release of classified information to IAEA, as agreed upon by the U. S./IAEA Safeguards Agreement, will result in a net advantage to the national security interest of the United States. Furthermore, Article 5 of the U.S./IAEA Safeguards Agreement satisfies the criteria of Section (D)(2)(a) of this part. The criterion of Section (D)(2)(a) of this part has been waived by the Commission. (ii)

Responsibilities (3)

The Director, Office of International Programs (OIP), will determine that the furnishing of classified information will result in a net advantage to the national security interests of the United States. The

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

Responsibilities (3) (continued)

determination must be made with the concurrence of the Office of the General Counsel (OGC), DFS, and the responsible program office. OIP will consult with the Department of State and other agencies and departments, as appropriate, in making this determination. OIP also will initiate and coordinate the procedural process to implement the proposed classified information transfers.

Classified Information Exchange Agreements With Foreign Governments (a)

Before the development of an exchange agreement, DFS will determine whether an applicable government-to-government agreement exists between the United States and the foreign country involved. (i)

If ~~no~~ an agreement exists, DFS, with the assistance of OIP and OGC, will develop a separate classified information exchange agreement for each foreign government agency involved before initial transfer of classified information or before initial written or oral access. This information exchange agreement must specify the requirements necessary to ensure the security of the transferred classified information. The agreement will be compatible with the terms and conditions of existing government-to-government agreements applicable to the transfer of classified information. (ii)

The EDO shall execute the exchange agreement upon a finding that the recipient government will provide adequate protection of the classified information to be furnished. The Commission will be informed by OIP before the execution of any international agreement. (iii)

The Commission will approve any waiver of the required understandings identified in Section (D)(2)(a) of this part concerning the criteria specified. (iv)

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

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

Responsibilities (3) (continued)

Classified Information Exchange Agreements With International Organizations (b)

The release of classified information to international organizations, with the exception of the IAEA, will be addressed on a case-by-case basis for each transmittal, considering the particular reason for providing classified information. Therefore, before permitting representatives of international organizations (with the exception of the IAEA) access to classified information, DFS must be consulted. (i)

DFS will coordinate the matter with OIP, OGC, and others, as appropriate, and approve or disapprove the access. If the access is approved, DFS will provide appropriate guidance to effect access or transmittal. (ii)

Internal Procedures (4)

Transfer of Classified Information to Foreign Governments (a)

Security Assurance and Security Checks (i)

A security assurance must be required and a security check made regarding the original recipients of classified information. (*a*)

OIP will obtain the security assurance and the background and biographical data on NRC Form 70, "Request for Name Check," and submit this information to DFS with request that the appropriate security check be conducted. (*b*)

The EDO is authorized to waive the requirement for a security assurance and/or a security check for high-ranking foreign government civil or military representatives when necessary. (*c*)

Results of Security Checks (ii)

The existence of security assurances and the results of any security checks, when applicable, must be made a matter of record in DFS. DFS shall make available any derogatory information derived from security checks on a confidential basis to only the Director, OIP, and the EDO.

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

Internal Procedures (4) (continued)

Review of Documents To Be Transferred (iii)

Classified documents to be transmitted to foreign governments must be forwarded to DFS for review and transmission. (*a*)

The review must ensure that—(*b*)

- Each original recipient possesses a prescribed security assurance; a security check of each original recipient has been conducted; and the results of the security check are favorable or a waiver has been obtained. (*i*)
- The information transmitted is within the scope of the government-to-government agreement negotiated with the country concerned and the classified information exchange agreement negotiated with the foreign government agency to which the documents are being furnished. (*ii*)
- Concurrence in the legal aspects of the transfer has been obtained from OGC. (*iii*)

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

Accountability (iv)

A record of accountability of the information being processed for release must be maintained by DFS and by each NRC office or division proposing the release of classified nonmilitary information to foreign governments or concurring in the release. (*a*)

The record must include—(*b*)

- Identification of the exact information released or being processed for release (for documents, the date, title, name of originator, and classification) (*i*)
- Names and signatures of approving officials (*ii*)

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

Internal Procedures (4) (continued)

- Form in which information is released or will be released (e.g., oral or documentary) (*iii*)
- Date of release or contemplated release (*iv*)
- Identity of foreign government organization to which and original individual recipient to whom release is made or is contemplated (*v*)
- Security assurance and security check, when applicable, for each individual recipient (*vi*)
- Waivers exercised or requested, when applicable (*vii*)
- Statement that the information is based on data originated outside NRC, wherever applicable, and the identity of the originating organization (*viii*)
- Name of individual in other United States Government agency who has authorized release, if applicable (*ix*)

The office or division contemplating or making oral disclosures must furnish memoranda before and after these disclosures to the Directors of DFS and OIP, and to OGC. (*c*)

Preparation and Method of Transmission (v)

The preparation (including classification) and method of transmission of documents are specified in Part I(C)(7) of this handbook. Normally, documents intended for a foreign government will be forwarded to that country's embassy in the United States. Transmission of classified mail to foreign countries requires prior approval of the Director, DFS.

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

The transfer of classified information to international organizations, except IAEA (see item (c) below), must be handled in accordance with guidance from DFS.

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

Internal Procedures (4) (continued)

Transfer of Classified Information to IAEA (c)

Written Disclosure Authorization (i)

A written disclosure authorization from DFS is required before IAEA representatives may have access to National Security Information. This authorization states that the individual is an authorized IAEA representative and is authorized to make visits or inspections in accordance with the U.S./IAEA Safeguards Agreement. (*a*)

The authorization includes—(*b*)

- The identity of the authorized IAEA representative (*i*)
- Specific authority to disclose National Security Information to that individual relating to the visit or inspection (*ii*)
- The level of classified information authorized (*iii*)
- A description of the IAEA representative's identification documents (*iv*)
- The purpose of the visit or inspection (*v*)
- The duration of the authorization to receive the information (*vi*)

In accordance with authority set forth in the disclosure authorization, classified documents may be furnished to IAEA representatives for retention or may be transmitted to IAEA. (*c*)

Review of Documents To Be Transferred (ii)

Classified documents to be furnished to IAEA representatives by approved means, or transmitted to IAEA representatives, must be reviewed by DFS before release. The review must ensure that the information to be furnished or transmitted is within the scope of the written disclosure authorization. (*a*)

If access or transmission involves classified information originated by another department or agency, DFS will obtain approval from the department or agency before access or transmission. (*b*)

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

Internal Procedures (4) (continued)

Accountability (iii)

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

Preparation and Method of Transmission (iv)

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

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

DFS will report to the NDPC those transfers of classified information to foreign governments or international organizations that must be reported under the national disclosure policy. This reporting is required in every instance in which defense information is involved.

Review and Concurrence in Legal Aspects of Transfer (vi)

OGC will review and concur in the legal aspects of NRC transfer of information to foreign governments or international organizations.

Access Lists (5)

Access to Top Secret information and NSCI requires a "Q" clearance, need to know, and the written authorization of the regional administrator or the director of the office sponsoring the activity or in which the individuals seeking access are employed. Each region and office with personnel authorized access to Top Secret information or NSCI will maintain a list of its authorized personnel. (a)

A copy of the access list for each region and office must be provided to DFS. Additionally, a copy of the NSCI access list for each region and office must be distributed in accordance with Part III(C)(2) of this handbook. (b)

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

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

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

Sanctions (6)

NRC employees, NRC contractors, and other organizations associated with the NRC program shall be subject to appropriate sanctions if they—(1)

- Knowingly, willfully, or negligently disclose to unauthorized persons information properly classified under EO 12958 or predecessor Executive orders, or the AEA. (a)
- Knowingly and willfully classify or continue the classification of information in violation of EO 12958 or any implementing directive. (b)
- Knowingly and willfully violate any other provision of EO 12958 or any implementing directive, or the AEA relating to the classification and declassification of Restricted Data and Formerly Restricted Data. (c)

Sanctions may include reprimand, suspension without pay, removal, termination of classification authority, loss or denial of access to classified information, or other sanctions in accordance with applicable law and NRC regulations. (2)

Classified Conferences (E)

Conferences and Symposia (1)

At times, NRC employees, NRC contractors, and other organizations affiliated with NRC sponsor or participate in conferences and symposia that are intended to be unclassified but that relate to sensitive programs or installations and may contain classified information. To minimize the risk of inadvertently revealing classified information at these meetings, the procedures below have been established.

- Papers involving sensitive programs or installations are to be submitted to an NRC authorized classifier (see Part I (B)(2) of this handbook) or to DFS for review before unclassified use. (a)

Classified Conferences (E) (continued)

Conferences and Symposia (1) (continued)

- All NRC and NRC contractor personnel who are to deliver briefings that involve sensitive programs or installations shall have the text of such briefings reviewed for classification by an NRC authorized classifier or by DFS before presentation. (b)

Publication or Release of Documents (2)

When there is doubt as to whether a document contains National Security Information, Restricted Data, or Formerly Restricted Data, the author shall refer the information to the appropriate NRC authorized classifier or the Director, DFS, for a classification review.

Review of Documents (3)

An NRC employee, an NRC contractor employee, or another person associated with the NRC program may desire to release, as unclassified, information relating to his or her activity. Contracts for classified work contain clauses that require safeguarding of classified information. To ensure that classified information is properly safeguarded, proposed disclosures, whether in the form of documents, visual materials, speeches, or otherwise, must be reviewed by an authorized classifier to prevent the inadvertent disclosure of classified information, as well as to obtain appropriate review for patent clearance. NRC employees and other personnel associated with the NRC program are under similar obligation to protect classified information against disclosure in conjunction with the release of unclassified information.

Review of Documents Submitted by Uncleared Authors (4)

Documents submitted for review by an uncleared author who, to the best of the reviewer's knowledge, has never had access to classified information, must be forwarded to DFS for review. If, after review, it is determined that the article contains information that should be classified, DFS will advise the author, to the extent possible within the bounds of security, of the reason for the classification and, if possible, take action to have the author delete any classified information contained in the document. In the course of such a review, DFS will refer the document to other NRC offices, to the NRC regions, and to other Government agencies, as appropriate.

Classified Conferences (E) (continued)

Review of Documents Submitted by Formerly Cleared Persons or by Authors With Active Clearances (5)

Documents submitted by persons formerly cleared at the "Q" or "L" level, by persons with active NRC clearances other than those set forth in MD 12.3, "Personnel Security Program," or by persons formerly or currently cleared by other Government agencies must be reviewed by an NRC-authorized classifier or by DFS. The author shall be required to delete any classified information in the document before it is published.

Transporting Classified Material via Commercial Airlines (F)

Approval for NRC contractor employees to hand-carry classified documents during travel via commercial airlines must be obtained from the Director, DFS. Additionally, the Federal Aviation Administration (FAA) has issued regulations for screening travelers and matter transported by air. Accordingly—(1)

- Each NRC employee and NRC contractor employee hand-carrying classified information shall carry his or her travel authorization and his or her NRC identification badge, which has his or her photograph and signature. The employee shall also carry the document authorizing him or her to hand-carry the information. (a)

- All passengers and items transported must be screened before boarding an aircraft. Briefcases or other luggage, including that containing the classified information, may be opened by airport screening personnel for inspection. This inspection must be conducted without opening the envelopes containing classified documents. The screener should be able to inspect the envelopes by flexing, touch, weight, x-ray, and so forth. (b)

- If the screener is not satisfied, the passenger will state that the packages contain classified information. The passenger will present his or her identification card and travel authorization. If the screener is still not satisfied, the passenger should immediately ask to talk to the senior air carrier representative or FAA security representative and explain the situation. If necessary, the traveler will contact his or her own supervisor or DFS. (c)

Transporting Classified Material via Commercial Airlines (F) (continued)

- In instances in which classified documents to be transported are of a size, weight, or shape not suitable for the processing specified above, the following procedures apply: (d)
  - NRC employees or NRC contractor personnel who have been authorized to transport classified documents must notify airline officials at the point of origin and at intermediate transfer points in advance of the trip. (i)
  - Employees carrying packages must report to the airline ticket counter and present documentation and a description of the containers that are exempt from screening. (ii)
  - Employees must have the original correspondence signed by appropriate supervisory personnel authorizing them to carry classified documents. This correspondence must be prepared on letterhead stationery of the NRC or the contractor employing the individuals. (iii)
  - Employees shall have enough authenticated copies of this correspondence to provide a copy to each airline involved. (iv)

The correspondence authorizing an employee to transport classified documents must contain—(2)

- The full name of the employee and the NRC office or the NRC contractor by whom employed (a)
- A description of the type of identification the employee will present (e.g., NRC photo badge) (b)
- A description of the matter being carried (e.g., "Three sealed packages, 9 inches by 8 inches by 24 inches," and the names of the sender and the addressee) (c)
- Identification of the point of departure, destination, and known transfer points (d)
- Date of issue and the expiration date of the correspondence, which is not to exceed 7 days from the date of issue (e)
- Name, title, signature, and telephone number of official authorizing the employee to carry the classified documents (f)

Transporting Classified Material via Commercial Airlines (F) (continued)

- Name and telephone number of the NRC official or the NRC contractor official who can confirm the letter of authorization (g)

Each package or carton to be exempt from screening must be signed on its face by the official signing the correspondence. When an employee is required to transport classified packages on a return trip and the letter from his or her organization does not cover this return trip, a letter of authorization must be prepared on the letterhead stationary of the agency or the contractor being visited. (3)

Exhibit 1

Required Markings for Classified Documents

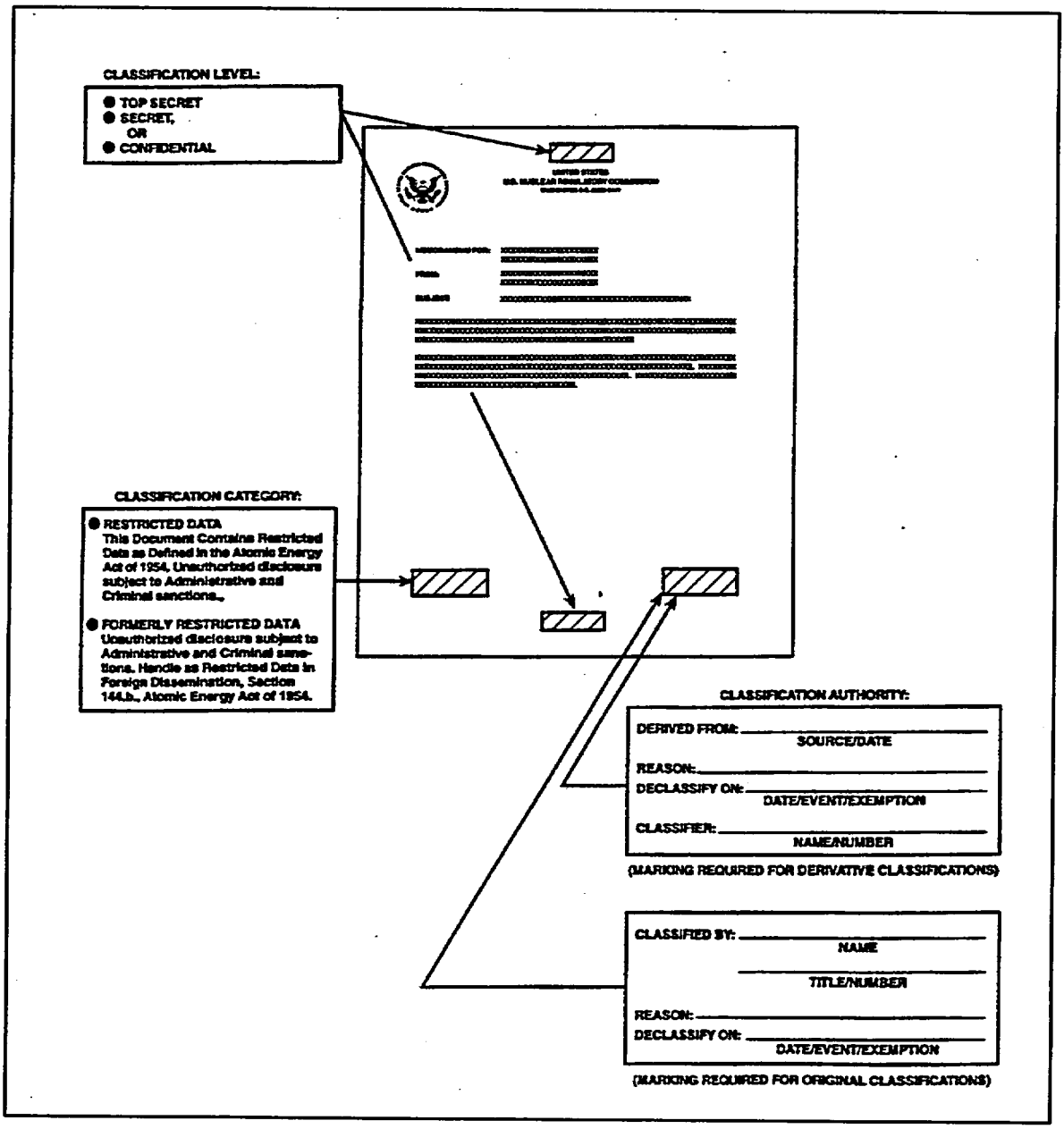


Exhibit 2

Declassification Markings

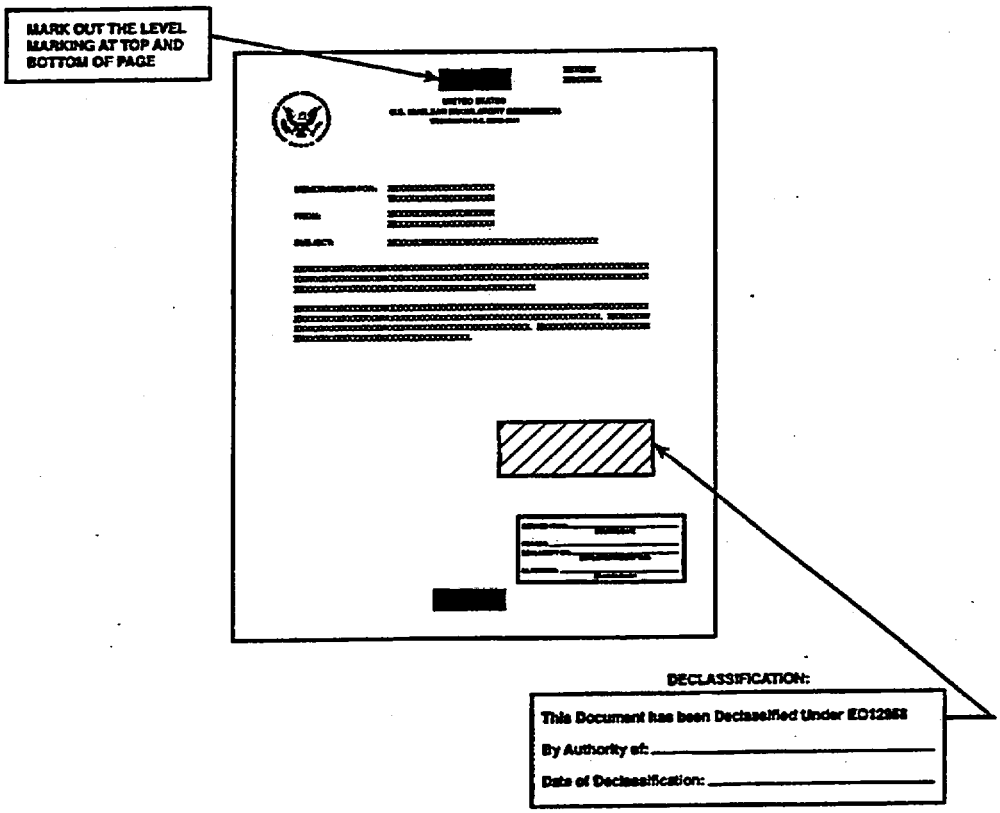


Exhibit 3

Subject or Title Marking and Portion-Marking

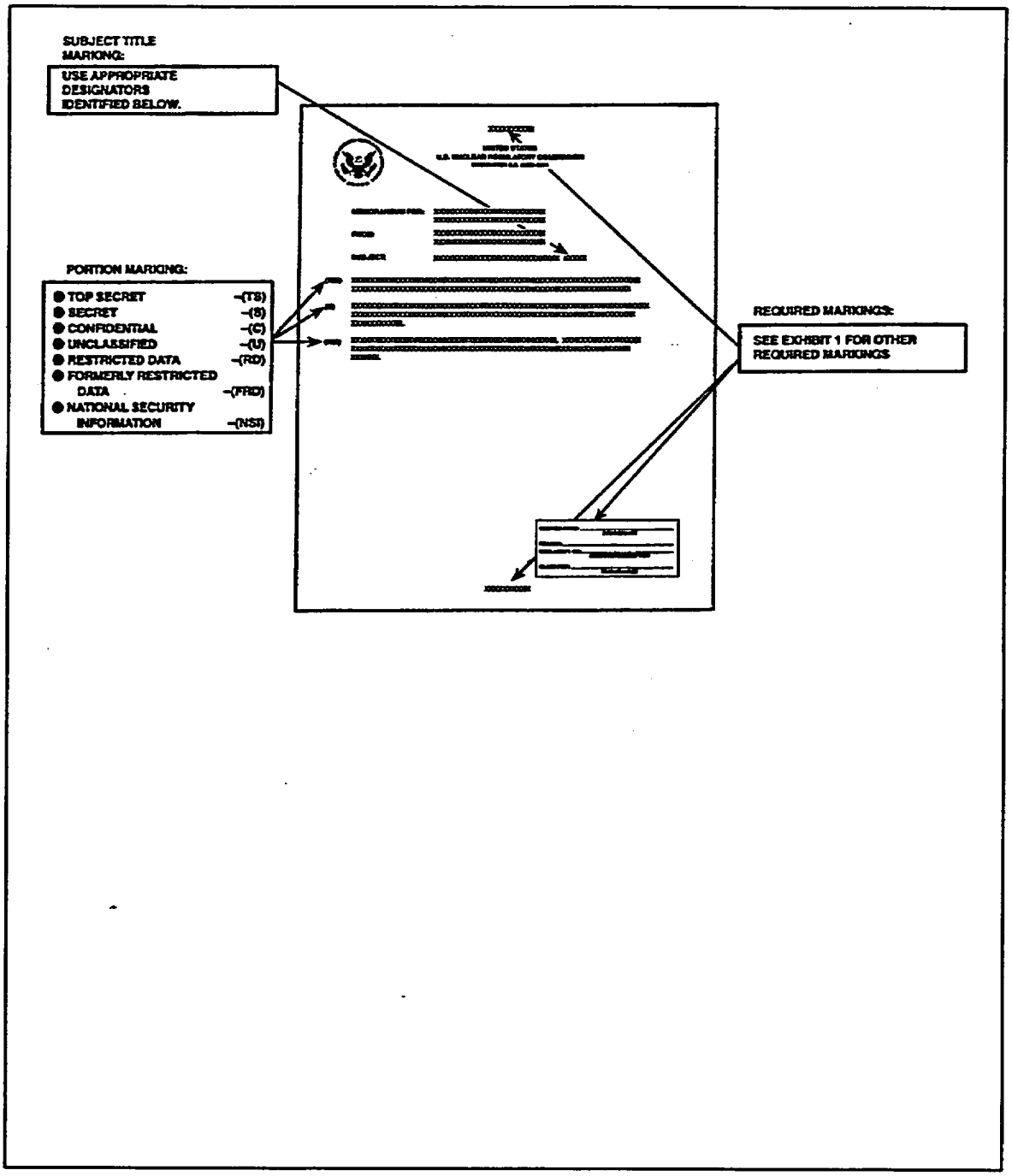


Exhibit 4

Upgrading, Downgrading, and Transclassification Markings

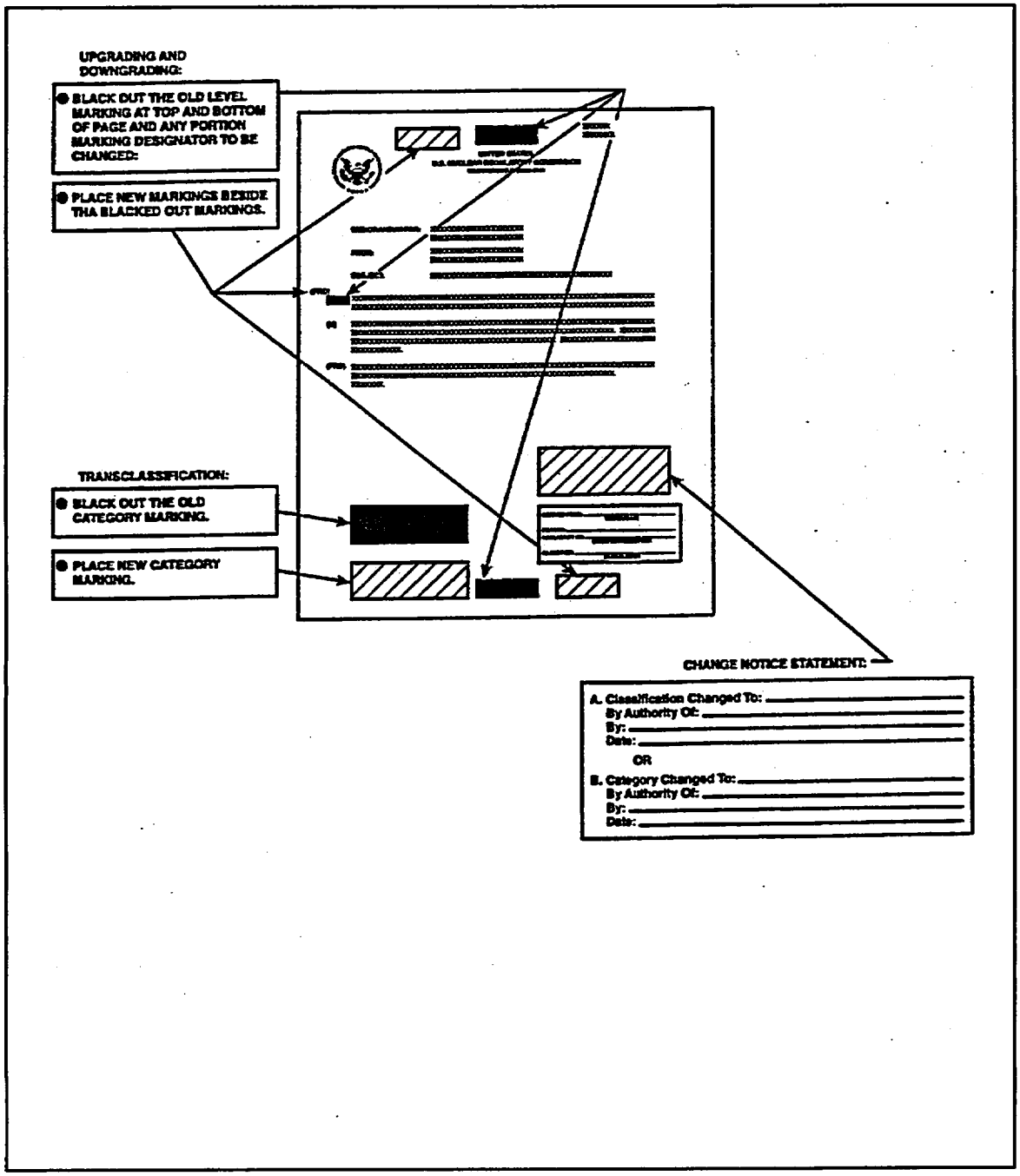


Exhibit 5

Deleting Classified Information From Classified Documents

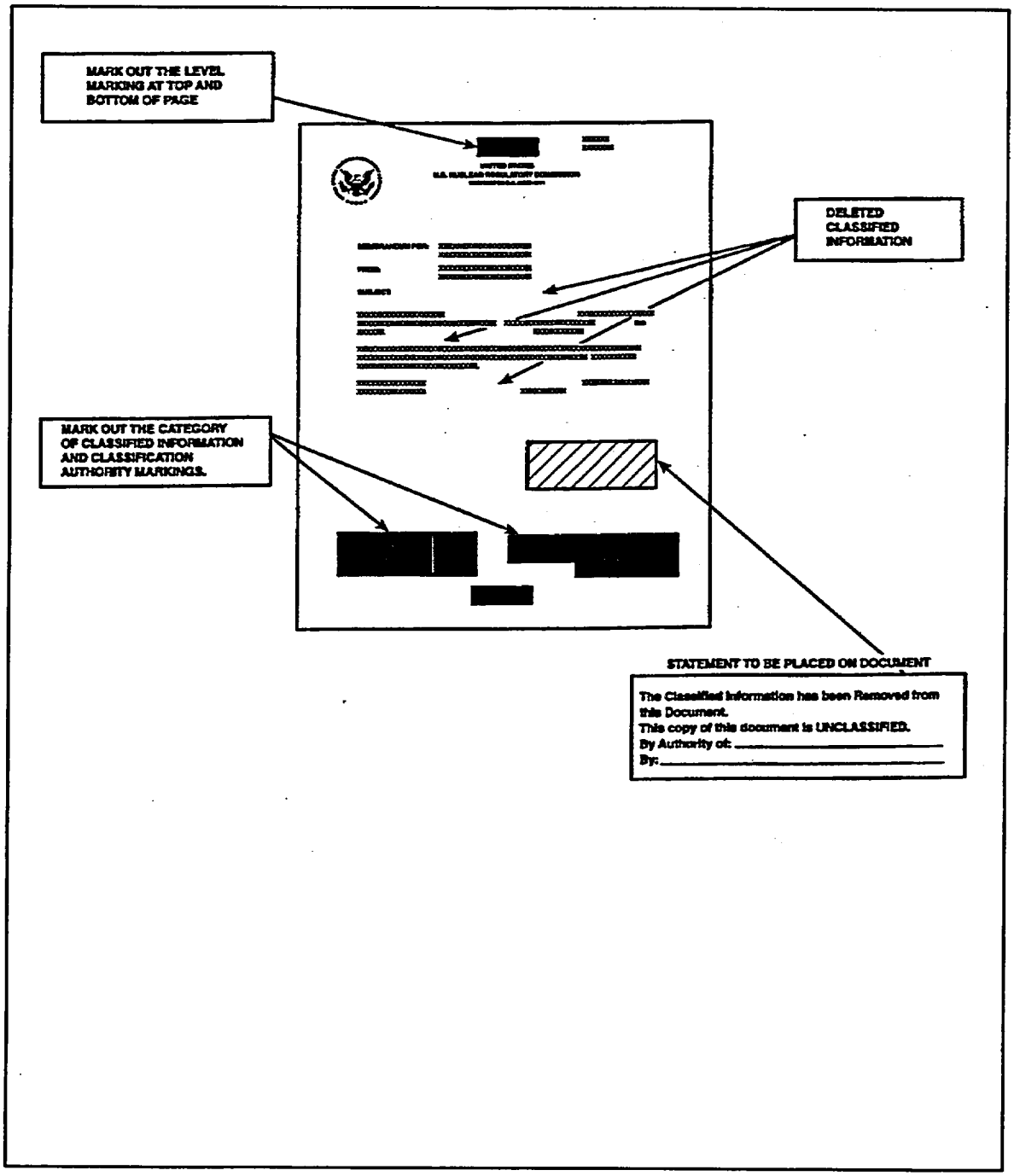


Exhibit 6

Required Markings for Unclassified Transmittal Document

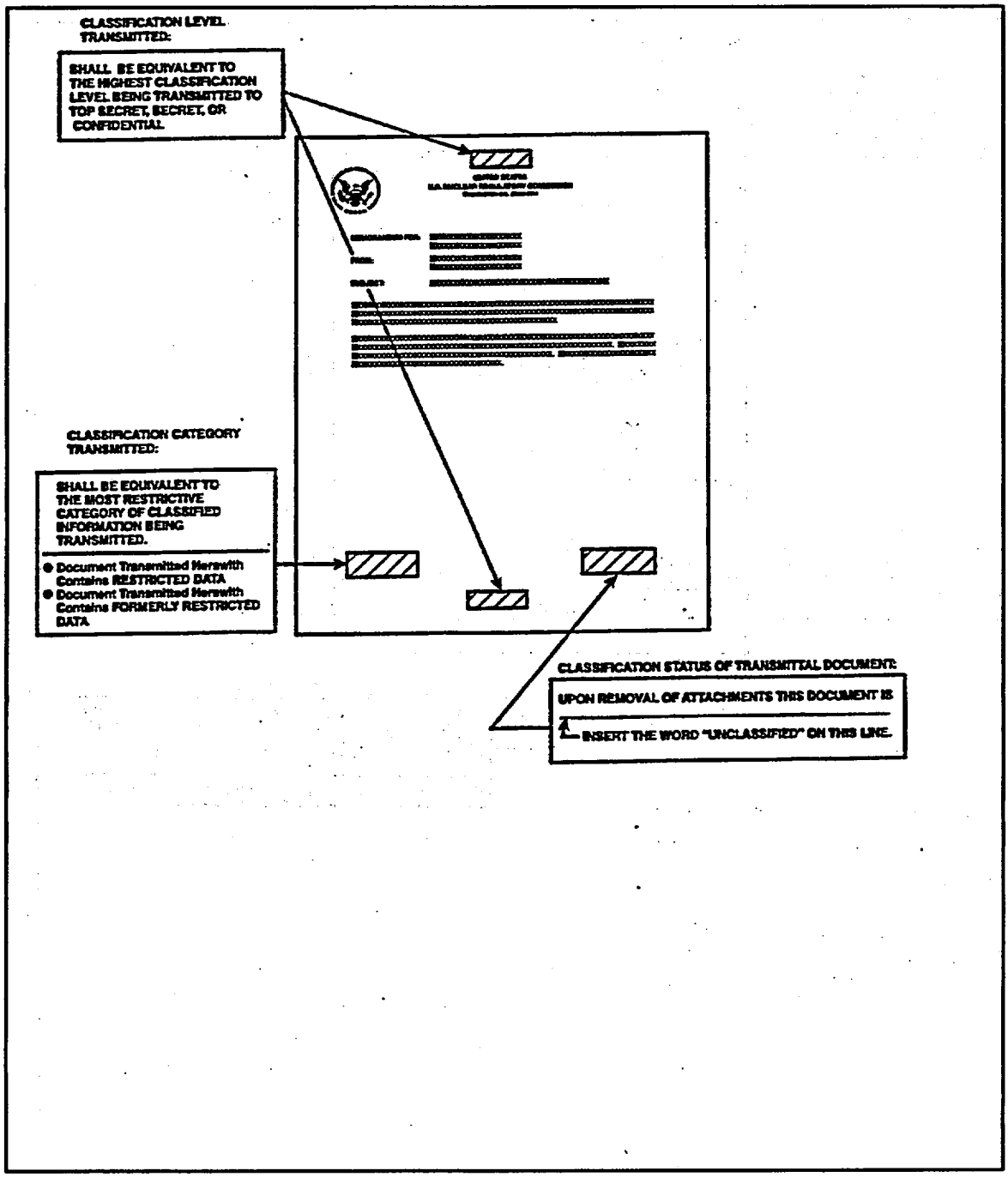


Exhibit 7

Required Markings for Classified Transmittal Document

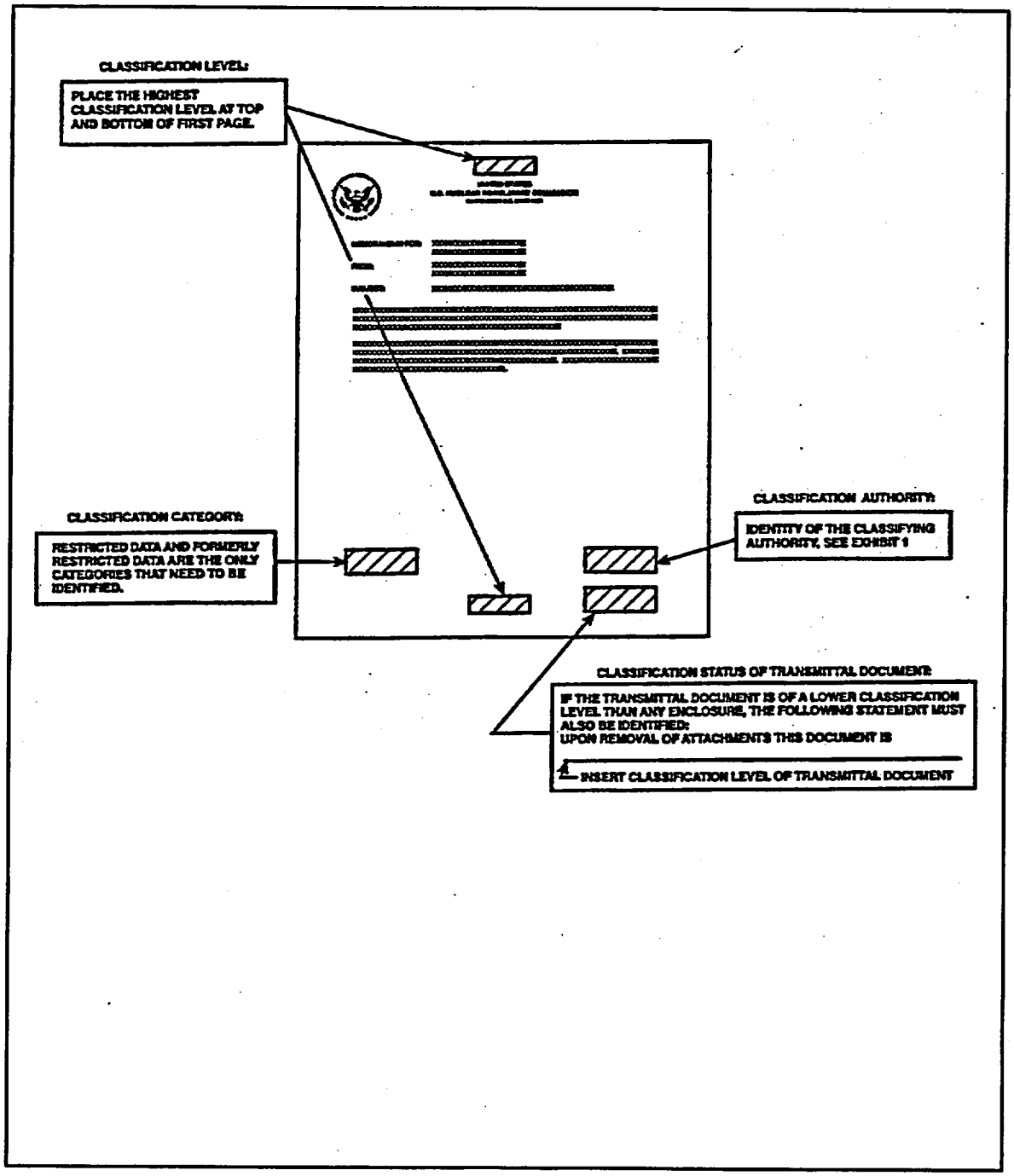
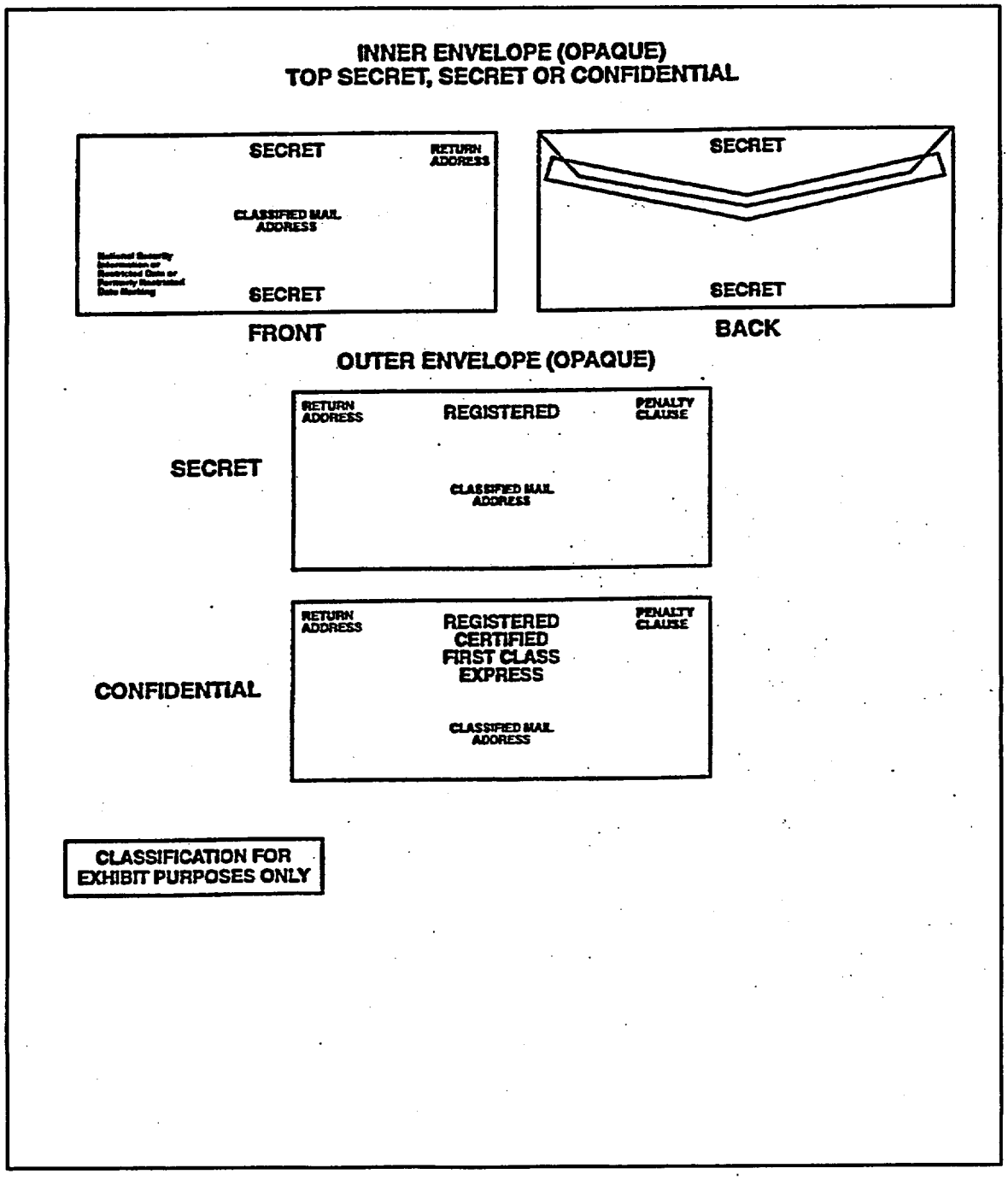


Exhibit 8

Required Markings for Envelopes or Wrappers